In The Balance

Toward a Model for Public Stewardship of Electronic Government Records

Final Report of the
Governor's Work Group on

Commercial Access To Government Electronic Records

November 1996

This document is available in alternative formats through the DIS Human Resources Office at 1110 Jefferson Street S.E., P.O. Box 42445, Olympia, WA 98504-2445. Or call 360/902-3543, TTY/TTD 1-800-883-6388.

To obtain a copy of this report, or its companion *Agency Survey Results*, please contact the Department of Information Services Communications Office at 360/407-4DIS (4347), by FAX at 360/438-7996, or via the Internet at contact@dis.wa.gov.

The *Final Report of the Governor's Work Group on Commercial Access to Government Electronic Records* and its companion documents are also available on the World Wide Web at http://www.wa.gov/dis/commaccess.

Printed on
Recycled Paper

STATE OF WASHINGTON

DEPARTMENT OF INFORMATION SERVICES

Olympia, Washington 98504-2445

December 9, 1996

The Honorable Mike Lowry, Governor

Dear Governor:

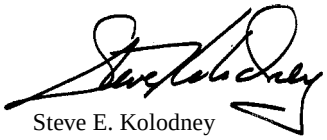
On behalf of the Governor's Work Group on Commercial Access to Government Electronic Records, I am pleased to present to you our final report, *In The Balance: Toward a Model for Public Stewardship of Electronic Government Records*. As the name suggests, the purpose of this report is to provide background, analysis and a balanced framework for a consistent statewide approach to commercial access to electronic government records.

On March 31, 1996, you called on members of your Executive Cabinet, together with members of the Legislature, to examine current practices and policies with a view to bringing consistency to the circumstances under which the state releases government records for commercial or business purposes. In your veto messages on House Bills 2790 and 2604 that created the Work Group, you were particularly concerned with safeguarding personally identifiable information and public stewardship — that is, deriving public benefit from the use of the state's information resources.

Those concerns have been borne out repeatedly during the Work Group's brief tenure. In a world driven by the relentless advancement of technology, where digital information now "commingles effortlessly," some have suggested that people have become numbed to the use of their personal information given over to the government. Citizens have told us that is not true. Their message is clear — they do not want information that the government collects about them used to monitor their behavior or intrude into their everyday lives.

We believe the recommendations for administrative and legislative action contained herein strike the correct balance between the citizens' expectations of safeguards of their personally identifiable information, the stewardship responsibilities of government and a defined sphere of legitimate business purposes. We trust that our findings will be useful to both the executive and legislative branches — and serve the best interests of the public in the emerging digital environment.

Sincerely,



Steve E. Kolodney
Chair, Governor's Work Group on
Commercial Access to Government Electronic Records

Membership of the Work Group

Steve E. Kolodney, *Chair*
Director
Department of Information Services

Katherine Baros Friedt
Director
Department of Licensing

Kent Caputo
Legal Counsel
Office of the Governor

Chip Holcomb
Senior Counsel
Office of the Attorney General

Dennis Karras
Director
Department of Personnel

Bruce Miyahara
Secretary
Department of Health

Gary Moore
Commissioner
Employment Security Department

Lyle Quasim
Secretary
Department of Social and Health Services

Nancy Zussy
State Librarian
Washington State Library

Legislative Members

The Honorable George Sellar
Washington State Senator

The Honorable Mary Margaret Haugen
Washington State Senator

The Honorable Philip Dyer
Washington State Representative

The Honorable Cathy Wolfe
Washington State Representative

Executive Summary

Public Policy Framework and Recommendations

I. Introduction: A Fundamental Shift

The constant evolution of technology presents a challenge for state agencies responsible for maintaining and releasing public records. Digital technologies create a fundamental change in the nature of records themselves, serving to expand the market for information, and increase the demand for government records in electronic format for a wide range of commercial purposes.

Some of the most valuable records include personally identifiable information about citizens, such as names, addresses and Social Security numbers. Commercial use of personally identifiable information contained in electronic public records raises new concerns about citizens' privacy in an electronic era.

The issues associated with the emerging online environment and the malleability of digital records came to a head when Governor Mike Lowry vetoed two bills passed by the 1996 Legislature. In his veto messages, the Governor announced the creation of a joint executive-legislative work group. That group, the Governor's Work Group on Commercial Access to Government Electronic Records, was to examine how government should manage records in the emerging electronic environment in a way that balances proper public stewardship, legitimate business use and safeguards for personally identifiable information.

In response, the Work Group is recommending enhanced protections for the privacy of the subjects of government records, guidelines for determining which commercial uses of public records should be prohibited, and protection for the public investment in information systems and software. As detailed below, the Work Group is asking the Legislature to delineate between legitimate business use and unauthorized commercial use, provide disincentives against inappropriate commercial use of electronic records, and allow agencies to recover a reasonable share of the cost of providing enhanced electronic access to these records.

II. Context

Government often serves a thermostatic function, balancing any number of competing, legitimate interests. The primary function of a thermostat is to maintain equilibrium in a changing environment. In essence, that was also the task given this Work Group by the Governor in March 1996. The changes of greatest interest here are threefold. First, digital technology brings with it a fundamental shift in records management (in both the public and private sectors) because once-discrete records can be "commingled effortlessly."[1] Second, the relationship between the public and private sectors is changing as government increasingly relies on the private sector to further public missions on its behalf. Third, the apparent implications of the technological and organizational changes have not been lost on the public. While some pundits suggest an eventual erosion in public expectations about privacy in the digital age, the overwhelming response in public comment to the Work Group is that government must take measures to safeguard personally identifiable information in the new networked environment.

The Work Group sought to address these changes by developing a framework for the stewardship of electronic government records that balances the needs of the public, the government and business interests. The Work Group endeavored to stay focused on issues related to commercial access. To do otherwise would have been a disser

[1] Nicholas Negroponte, *Being Digital*, New York, Albert A. Knoff, 1995:18.

vice to the wider concerns on which it touched and the people who have dedicated much time, attention and thought to them.

The Work Group seeks to reinforce the spirit of the Open Records Act by updating the letter of some its provisions. The rise of digital technologies has made it necessary to refresh how the law works in some narrow, specific areas where, in the Work Group's view, its provisions do not lend themselves to a digital, networked environment.

To be clear in establishing the context for the discussion and recommendations that follow, the Governor stated at the outset that "the work group will not consider media access to government records in electronic format as a commercial use when such access is being requested for reporting purposes." For the purposes of the Work Group, newsgathering is analogous to public access and is not addressed directly by the current study.

III. Policy Framework

The Work Group's proposals are anchored in the 10 principles articulated here as a policy framework within which decisions concerning commercial access to government electronic records should be made.

Principle 1

Digital technology changes the nature of public records themselves, bringing with it the prospect for greater governmental efficiencies and the need for additional safeguards to protect personally identifiable information.

Principle 2

Public records are a public trust. The ownership of those records should not be transferred to other parties. The universe of public records subject to disclosure is defined by statute.

Principle 3

The highest public benefit from public records is when they are used to further a public mission. The public-benefit test of remaining within their "original orbit" — that is, use that advances an agency's public mission — is useful in determining legitimate governmental or business uses of information.

Principle 4

Government has a duty to safeguard the personally identifiable information of ordinary citizens from abuse. The duty extends to the notification of individuals of the procedures in place for the inspection of information held about them.

Principle 5

Policies to safeguard personally identifiable information must balance business and government needs for access to information with an individual's expectations of privacy.

Principle 6

Government should not restrict access to information about the performance of public institutions or about public policy.

Principle 7

The public should not have to pay to inspect information collected by government at taxpayer expense.

Principle 8

Financial disincentives should not be used to restrict access to government information.

Principle 9

Cost recovery for commercial access should be based on providing enhanced access, not the "selling" of public records.

Principle 10

Agencies should not be required to provide enhanced electronic delivery of information for commercial or business purposes unless they can charge fees to recover a reasonable portion of the costs of developing and maintaining information systems.

The 10 principles informed the group's deliberations and shaped the resulting themes, findings and recommendations.

IV. Major Themes

The Work Group's findings are best understood in the context of three major themes:

Legitimate Business Uses vs. Prohibited Commercial Uses

There is a legitimate public interest in certain business uses of government records that further a public mission and improve decision making in both the public and private sectors.

Safeguards on Personally Identifiable Information

It is the stewardship responsibility of those entrusted with personally identifiable information to safeguard it from abuse. Safeguards are ineffective without clearly articulated penalties which should include both financial disincentives and the loss of access to government records.

Public Stewardship

Government records and the systems and software that maintain them in electronic form represent a significant public investment which should be managed accordingly. Government adds value to the records it collects by perfecting data through continual updates, indexing and other measures. Taxpayer subsidies of commercial access should redirected to support public access and infrastructure refurbishment.

There is a dynamic tension between some elements of these themes which the Work Group has sought to balance.

V: Findings and Recommendations

Legitimate Business Uses vs. Prohibited Commercial Uses

In assessing the circumstances under which government records in electronic format should be released for commercial, profit-making purposes, the Work Group examined practices and policies in other jurisdictions, surveyed state agencies and local governments[2] in Washington State and consulted with a number of interested parties and area experts.

The Work Group took testimony from legal counsel for The Seattle Times on behalf of the larger newspaper industry, legal counsel for an industry and creative group representing the emerging new media, and representatives of the commercial information reselling sector — Commercial Information Systems (CIS), Inc., The Polk Company and Automated Systems Inc.[3] The testimony of the resellers was supported by written submissions from 28 companies that rely on resellers to conduct business and comply with legal or regulatory requirements.[4]

[2] Local government was represented by the Association of Washington Cities and the Washington Association of County Officials.

[3] See Appendix A.

[4] See Appendix B.

Information required to meet regulatory requirements or conduct business in a safe and legal manner is defined by the Work Group as "legitimate business use." The Work Group believes such business purposes should be delineated in statute from commercial purposes, which are defined as commercial contact for profit-making purposes.

Findings:

- Many companies rely on a third party to corroborate information given to them by applicants and customers in the legitimate conduct of their business.
- Such verification is often needed to comply with government regulations.
- Government records are used to verify certain information in order to conduct business in a legal and responsible manner.
- Government has a duty to release the information needed to comply with obligations it imposes on the private sector.
- Permissible business use should meet a test of demonstrable public benefit.
- The use of government records for "legitimate business purposes" needs to be distinguished from "commercial purposes" as used in the Open Records Act.
- Current restrictions on "commercial use" — defined by the Attorney General as direct contact for profit-making purposes — should be maintained.

Recommendations:

Statutory Definitions of Business and Commercial Purposes

> The Work Group recommends that the Legislature distinguish in statute between commercial and business purposes. Such a distinction would allow legitimate business use of government records to further a public purpose while maintaining restrictions on secondary use that provides no public benefit.

The Work Group's recommendations concerning the circumstances under which government records in electronic format should be released for business or commercial purposes are discussed fully in Chapter 3.

Safeguards on Personally Identifiable Information

The Work Group sought public comment on its work and the issues before it. With few exceptions, the public comment focused on safeguarding personally identifiable information in a networked digital environment. It was apparent that the concerns of citizens were being informed by a wider set of developments — that is, revelations about the impact of advanced information technologies on their lives and their privacy. In the seven months since the Governor announced the creation of the Work Group, a steady series of over 100 news stories has illustrated the ever-increasing scope of the issues identified in the veto messages.

To further explore concerns regarding personally identifiable information, the Work Group brought representatives of the commercial resellers together with privacy experts and advocates. Building on the previous testimony from parties named above, the Legislative Director of the American Civil Liberties Union (ACLU) of Washington and a

member of the Public Information Access Policy Task Force added to the Work Group's understanding of the privacy concerns associated with commercial access to digital records. Dr. Ann Cavoukian, author of Who Knows: Safeguarding Your Privacy in a Networked World, joined the Work Group via a videoconference to discuss — among other things — privacy protection as a competitive advantage in the private sector.

Findings:

- The Open Records Act provides that all public information, including personally identifiable information, is subject to disclosure unless specifically exempted.
- The Open Records Act is silent on sanctions against improper initial release of public records — and on misuse related to secondary use.
- The public expects government to safeguard its personally identifiable information from inappropriate use.
- Privacy protection can be a competitive advantage in the private sector.
- Private-sector industry groups have responded to public concern by introducing voluntary codes of practice to protect privacy.
- The collection of personally identifiable information should be limited to that which is necessary to fulfill legislative mandates of respective agencies.
- Any public records released for business purposes should be limited to targeted use within their original orbit — that is, use that furthers a public purpose.
- Contractual obligations with information resellers can increase accountability for unauthorized use.
- Loss of access may be a more effective disincentive than monetary penalties alone.
- Flexibility in the handling of personally identifiable information to meet a variety of access circumstances should be a basic and ubiquitous requirement for new-systems design and for major system upgrades.
- Beyond issues related to personally identifiable information, proprietary business information provided to government as a condition of license or reporting requirement is treated unevenly from agency to agency. Such information may be exempt from disclosure under statute at one agency but open to disclosure at another, leaving the business at a potential competitive disadvantage.

Recommendations:

Public Notice

The Work Group recommends that agencies post and/or publish public notice that the information gathered is subject to disclosure for those purposes allowed in statute. The agency-specific public notice should reflect the common uses of such records. The public notice should also provide information about the procedures in place for the inspection by individuals of information held about them, pursuant to RCW 43.105.310.

Statutory Definitions

To better reflect the realities of the digital environment, the Work Group recommends that the Legislature clarify the language in the Open

Records Act by amending RCW 42.17.260(9) from "list of individuals" to "personally identifiable information."

The Work Group further asks the Legislature to provide additional guidance to state agencies by adding a definition in the Open Records Act of inappropriate commercial use of personally identifiable information.

Disincentives

The Work Group recommends that the Legislature authorize disincentives to abuse of information contained in records released under the Open Records Act. The Work Group believes the best alternative is in practical remedies that safeguard personally identifiable information — rather than the criminalization of unauthorized use.

To that end, the Work Group recommends that the Legislature include provisions that permit agencies to detect unauthorized use. Commonly referred to as "salting" or the use of "tracers," the practice should be supported by an audit provision.

The Work Group further recommends that penalties for abuse be clearly articulated in statute and in contracts with private-sector resellers (or other such vendors). The penalties favored by the Work Group are monetary penalties (on a per-record basis) and, more importantly, the loss of access in cases of demonstrable abuse.

Governor's Directive

The Work Group asks the Governor to issue an Executive Order that instructs state agencies to adhere to a model contract for the release of information for commercial purposes. Such a contract will specify the specific business purposes for which the released records could be used, the necessary safeguards for personally identifiable information (salting and auditing) and the penalties for their unauthorized use.

The model contract between a public entity (agency) and a contractor (private-sector reseller or vendor) should be characterized by the following:

- specific contractual limitations on acceptable use, consistent with a record's "original orbit" and a public purpose.
- specific contractual requirements to safeguard personally identifiable information, including the contractor's adherence to current or amended provisions.
- specific contractual requirement for the contractor to obtain prior written approval for any use outside of those specified in contact.
- specific contractual provision that no personally identifiable information furnished by the public entity to the contractor be published by the contractor in any manner, or be used for unsolicited commercial contact.
- specific contractual provisions under which the contractor assumes responsibility to ensure that any personally identifiable information under contract is used only for the specified purpose.
- specific contractual provisions under which the contractor agrees to "salting" and auditing provisions to detect abuse of personally identifiable information contained in public records.
- specific clauses that prevent contract assignment and deny the creation of proprietary rights to the information by the contractor.
- specific contractual language that establishes broad grounds for contract cancellation by the public entity.
- specific contractual language that permits unrestricted remedies on the part of the public entity, including but not limited to loss of

access and financial penalties (on a per-record basis).

- specific contractual language that establishes a security deposit against which financial penalties will be drawn.

Proprietary Business Information

Fully one third of the exemptions of the Open Records Act address the commercial sector. Following on the Work Group's efforts to develop a framework for the consistent handling of personally identifiable information in areas related to commercial access, the group also encourages the Legislature to bring uniformity to the handling of proprietary business information.

> The Work Group recommends that state law and practices concerning the disclosure of proprietary business information be made more consistent across agencies. Businesses should not be placed at a competitive disadvantage due to uneven disclosure provisions associated with state regulation and reporting requirements.

The Work Group's recommendations concerning safeguards for personally identifiable information and disincentives for abuse of such information are discussed fully in Chapter 4.

Public Stewardship

In the view of the Work Group, taxpayers should not subsidize profit-making activities. Therefore, agencies should be able to charge fees for enhanced electronic commercial access to recover a reasonable portion of the costs of developing and maintaining information systems.

The Work Group held a wide-ranging discussion of cost recovery mechanisms with the assistance of representatives of CIS and Polk, together with John Doktor from The Public Sector Marketing Group, Inc. and Dr. Mark Haselkorn, Chair of Technical Communications in the College of Engineering at the University of Washington.

Findings:

- government must be deliberate in developing a model for cost recovery that provides for sharing risks and sharing rewards.

- government is not a passive holder of information, but a development environment which adds value to the information that is ultimately of commercial or business interest.

- repurposing of government records by business or commercial interests must be consistent with a legitimate public purpose.

- providing low- or no-cost access to commercial enterprises would effectively provide a substantial and largely invisible taxpayer subsidy of those enterprises — even where most taxpayers will not use the electronic services and thus receive no offsetting public benefit.

- the marginal costs to business of enhanced electronic access to government records often reduce the cost of doing business for private-sector enterprises.

- public-private partnerships, where the value added by both partners is recognized, may be an effective means to recoup taxpayer cost which would otherwise be provided as subsidies to commercial enterprises.

- the Open Records Act does not distinguish between public records and the software that creates and maintains them in a digital environment. In the absence of any protections for the significant public investment in proprietary software, the state faces difficulties in ensuring the future availability, enhancement and refurbishment of these systems.

Recommendations:

Public-Private Partnerships

The Work Group urges the Legislature to protect, promote and maintain the significant taxpayer investment in the collection of public records and the infrastructure that supports them.

The Work Group urges the Legislature to encourage public-private sector cooperation in ways that further the public mission of the state, maintain and enhance public access to public information, and maintain equal commercial access for all businesses and resellers.

The Work Group recommends that any fee or pricing schedule for commercial access be based on allocating costs related to providing enhanced electronic access — not the 'selling' of public records.

The Work Group believes any future legislation concerning commercial access to government records should be characterized by the following:

- contracts with private sector vendor or partner be non-exclusive and short-term.

- ownership of the unique, authoritative records remain with the public entity.

- revenues from enhanced business access should be redirected to the support of public access systems and infrastructure refurbishment.

Software Exemption

The Work Group's primary focus was government's role in the stewardship of records in the digital environment and the legitimate business uses of government records that further a public purpose. Such a discussion necessarily touches on the digital environment itself — and how the software that creates and maintains the records is developed and refurbished.

State government spends millions of dollars in the development of computer software that supports the public missions of its agencies. This public investment is jeopardized because such software, under current law, can be defined as a public record, allowing private-sector companies to request copies of the software at the cost of duplication without contributing to its development costs.

The issue is further complicated in the case of public-private partnerships, where a private-sector firm agrees to share the risks and rewards of such a development project. The cost to the state is typically reduced under such arrangements, in exchange for a sharing of the intellectual property rights derived from the project. The state would be unable to provide sufficient protection of its partners' or its own rights to the software it develops so long as the software itself is considered a public record.

The Work Group recommends that Washington State make its policies regarding the development of proprietary software consistent with 22 other states with which it competes for private partners. To that end, the Work Group asks the Legislature to exempt software from the definition of a public record. In the Work Group's view, such an exemp-

tion should come with a caveat that makes copies of such software available in perpetuity for government purposes and public inspection of records (where allowed under statute).

The Work Group's recommendations concerning public stewardship and subsidies are discussed fully in Chapter 5.

Commercial Access To Government Electronic Records

Final Report

Table of Contents

Overview and Charter

Chapter 1

In 1972 the people of Washington State passed a citizen initiative to establish the Open Records Act. The Act provides broad access to government records to ensure the public's right to monitor government activities. The Act also recognizes the right of individuals to keep certain information private by prohibiting access to information "that is highly offensive to a reasonable person and of no legitimate public concern."

The intervening 24 years have seen the proliferation of exemptions to the Act. These exemptions, or authorizations, grew more frequent as records became available electronically. As the very nature of the records changed, so did the nature of the requests for public information. Requests for single or multiple records became requests for entire databases which could be used in ways not anticipated by the present law. The second and third use of these records became an issue — as did the sheer volume of records that were being released.

The Work Group is a narrowly focused response to a specific problem. On March 30, 1996, Governor Mike Lowry came to the defense of the Open Records Act by vetoing new bills passed by the legislature that, in the Governor's view, threatened to further erode the Act's provisions. In response to "serious questions [raised by the bills] that state policy now fails to answer," the Governor convened a Work Group to review current state practices and policies.

I. The Charter

The Governor gave the work group a carefully defined charter.

> The charter of the Work Group is to recommend whether and under what circumstances government records in electronic format should be released for commercial, profit-making purposes, with particular emphasis on safeguarding the privacy rights of individuals who are subject to those records.

Three questions that flow from the charter defined the work of the group.

Question 1: How, and under what circumstances, should public records in electronic format be released for business or commercial purposes?

Question 2: How can citizens be assured that personal information about them will be safeguarded when public records in electronic format are released for business or commercial purposes?

Question 3: If public records in electronic format are to be released for business or commercial purposes, how should the state allocate and recover costs?

The chapters that follow provide the Work Group's answers to these questions.

The Governor convened this work group to consider the limited question of the use of electronic government records for commercial purposes.

II. Background to the Work Group's Creation

The Work Group exists to carefully examine a thorny thicket of important and compelling issues:

> How does government conduct business in an emerging electronic environment in a way that ensures proper public stewardship on one hand and protection of personal privacy on the other?

The issues associated with the emerging online environment and the malleability of electronic records came to a head earlier this year with two bills introduced and passed by the 1996 Legislature. HB 2790 would have provided private com-

panies on-line, machine-readable access to state-agency computer files, only to have these companies sell that information back to the government for a profit.[5] HB 2604 would have given commercial parking companies electronic access to DOL records to facilitate the collection of parking fees.[6]

The Governor's vetoes also reflect what the Public Information Access Policy Task Force identified as "the public's concerns [that] may well warrant an evaluation of current processes, procedures, and laws related to public records — recognizing that the balance between public access and personal privacy is not fixed, but changes as technologies advance...."[7] In his veto message for HB 2604, the Governor wrote, "As state government responds to emerging technologies, it is likely that we will have to modify the way we control and disburse the information we hold. However, in order to protect the privacy of our citizens, we should change our policies with great care and only after the broadest possible debate."[8]

Issues related to public stewardship demand that the state examine its current practices in this area. The information technology (IT) that makes electronic access possible, and the records such IT systems hold, are public assets. As such, citizens should not pay twice for access to information they need to hold their government to account. At the same time, early adopters of electronic access to government information systems tend to be commercial interests which use the information for a profit-making purpose. As early adopters, they enjoy a substantial (and invisible) taxpayer subsidy of their enterprise while many citizens pay for a system they do not use.

The issues before the work group were not new but they cannot be ignored. The 1996 Legislature dealt with eight bills and a budget proviso that related to commercial access to government records. There is every reason to believe that the issues before the Work Group will be the subject of legislation in the 1997 session and beyond.

There was some initial concern that the Work Group is revisiting issues already addressed by the Public Information Access Policy Task Force, the final report of which was the basis of important legislation concerning the enhancement of public access to government records in the 1996 session.[9]

However, the Task Force conceded in its own final report that it was unable to bring full closure to a number of important issues. In fact, the Task Force urged the Legislature to "consider and resolve privacy issues which may not be resolvable within the current public records law." Further, it asked the Legislature to "clarify and resolve remaining cost, funding and fee issues."[10] In many ways, the Work Group was a response to those requests for further research and clarification, and fully supportive of the Task Force.

Rather than duplicate the work of the Task Force, the Work Group sought to continue the vital public conversation that the Task Force began. It is a conversation in which the Work Group included the voices of individuals from across the state, as well as organizations, educational institutions, privacy advocates and commercial interests. Supported by a site on the World Wide Web and a dedicated e-mail address, the Work Group sought public input regarding the important issues before it. The Work Group was also able to communicate directly with the public through gavel-to-gavel television coverage of its deliberations on TVW, Washington State's Public Affairs Network.

[5] The full text of HB 2790 and the Governor's veto message is provided in Appendix D.

[6] The full text of HB 2604 and the Governor's veto message is provided in Appendix E.

[7] Public Information Access Policy Task Force, *Final Report and Recommendations: Encouraging Widespread Public Electronic Access to Public Records and Information Held by State and Local Governments*, December 1, 1995, p. 30.

[8] *Veto Message on HB 2604*, March 30, 1996.

[9] RCW 43.105.270.

[10] PIAPTF, *Final Report*, p. 16.

The Current Landscape

Chapter 2

Overview Of Federal And State Policies And Practices

As a starting point, the Work Group set out to examine the current landscape of policies and practices in Washington State and elsewhere. The results of its review follow.

Changes in technology and in the potential commercial value of public records are creating new challenges for policy makers in every state and the federal government. All 50 states have in recent years adjusted the definition of "public record" to include electronic media. States are confronted by the increasing commercial value of information, especially personal information that can be used commercially in ways that compromise citizens' privacy. Another issue is whether access fees for electronic information should be based on the cost of providing the access, or on the market value of the information.

I. Washington State Current Practices Agency Survey

The Work Group conducted a survey of current agency practices related to commercial release of public records. The results are summarized below, based on an 80 percent response rate (41 of 51 agencies):

Holdings and Requests

- Seventy-nine percent (79%) of reporting agencies or jurisdictions collect, generate, or serve as a steward for confidential proprietary information, intellectual properties, or commercial information supplied by businesses or individuals.
- Eighty-five percent (85%) of agencies have received requests for data and/or systems for commercial purposes.
- Sixty-eight percent (68%) have received requests for litigation purposes.

Statutory Authority

- Seventy-two percent (72%) reported that such information was protected by a statutory exemption from disclosure, or exemption resulting from case law.
- Twelve percent (12%) of agencies reported they had specific statutory authority to release lists of personal information for commercial use.

Privacy

- Twenty-five percent (25%) of respondents reported that their agencies collected personal information from citizens that is disclosable for commercial purposes.
- Fifty-six percent (56%) of respondents said the state should place new limitations on the commercial use of personal information or databases containing personal information in state-controlled systems.
- Only two agencies reported that they inform citizens that the information may be used for commercial purposes.

Cost Recovery

- Thirty-eight percent (38%) of agencies have statutory authority to charge fees for cost recovery on a basis other than the incremental cost of copying.
- Of those agencies authorized to recover costs other than the incremental cost of providing a copy, additional charges were most often based on: 1) salaries, wages and benefits; 2) downloading/extraction to distribution media; 3) data compilation and processing; 4) all identifiable administrative costs; and 5) costs contracted out.

Technology

- Sixty percent (60%) of agencies have experienced difficulty in responding to requests for information that is stored electronically.

The Work Group has prepared a detailed summary of the survey results. It is published under a separate cover.

II. Policies to Recover Costs from Commercial Use of Public Records in Other Jurisdictions

Qualifying Users

The federal government and certain states have policies based on the *identity of the requester* of the information, or the intended use of the information. In some cases, these policies are designed to protect citizen privacy from intrusive commercial uses of public records, such as direct marketing (see Section III below). In other cases, the policies are to make commercial users pay more for access to public records than other requesters, on the grounds that the public resource of information should not be used to subsidize businesses, or simply to retain for the public some of the commercial value of the information.

The federal Freedom of Information Act (FOIA)[11] establishes a fee schedule that distinguishes between the media, educators and researchers (who pay the cost of duplication only) and commercial requesters (who pay additional search and review fees).[12] These provisions have not been challenged. However, at least one court has suggested that because commercial/non-commercial distinctions work to limit access to public data to commercial vendors, they raise potential First Amendment concerns.[13]

A recent survey by the National Conference of State Legislatures (NCSL)[14] found a number of states are using this type of fee schedule to raise revenue from commercial requests for electronic information. According to NCSL, seven states currently make such a distinction between commercial and non-commercial requests (Arizona, Idaho, Indiana, Kentucky, Minnesota, Oklahoma and Tennessee).

Another approach taken by many states is to withhold valuable software and databases from commercial users, often by removing "software" from the definition of public record, or by allowing agencies to copyright software they have developed with public funds. According to NCSL, 20 states have statutory provisions that exempt software in some way, and the attorneys general of Michigan, Mississippi and Nevada have issued opinions exempting government-developed software. Kentucky and certain local governments in North Carolina have laws allowing them to withhold public geographic information systems from commercial requesters. On the other hand, Alaska and Kentucky specifically include software in their statutory definition of "public record."

In some cases, the distinction is used to give lower-cost access to public information that is to be used for a public purpose such as research or education. Alaska, for example, allows a fee for electronic services or products to be waived if the service or product is to be used for a public purpose such as research or education.

Other states have a policy of prohibiting higher fees for commercial users. Some opponents to differential fees for commercial users argue that commercial users, as taxpaying members of the public, are already entitled to public information. Another argument against this practice is that it is difficult to verify the identify of a requester and that it can potentially be abused and have a chilling effect on public access. North Carolina and Ohio statutes specifically prohibit inquiry into a requester's intended use of public information.

[11] 5 U.S.C.A. Sec. 552

[12] House Committee on Government Operations. "A Citizen Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records." H.R. REP. No. 103-104, 103d Cong., 1st Sess. 9 (1993).

[13] *Legi-Tech v. Keiper*, 766 F. 2d 728 (2d Cir. 1985).

[14] Anneliese May. DRAFT: "Access to Electronic Public Information: A Summary of Current Trends." National Conference of State Legislatures (NCSL), July 1996.

Enhanced Access: Cost Recovery Trends in Access to Electronic Public Records

A growing number of states are basing cost-recovery fee schedules on a distinction based on type of service as opposed to type of requester or intended use. This type of distinction can be used in effect to charge commercial users at a higher rate, without the difficulty of verifying identity or motive. For example, a state could set higher fees for high-volume record requests, on the assumption that the high volume signals commercial intent, and yet retain the authority to waive the higher fee for requests intended for public purposes such as journalism or research.

Some states are treating "enhanced" electronic access (such as dedicated access lines, search capabilities for public databases, or customized records) as a source of revenue to recoup the cost of developing information systems or to support other government functions. Typically, states that offer enhanced electronic access for a fee also offer a certain amount of no-cost or nominal-cost electronic information. However, in some cases virtually all electronic access to public records is treated as an "enhanced" service and is made available only for a fee. Other states view fees as a barrier to public access and choose not to offer enhanced fee-based electronic services. In Florida, for example, statute allows agencies to recover costs from record requests but prohibits agencies from entering into contracts to sell access to public records.

A few examples illustrate the range of states' current policies for balancing cost recovery with public access. Alaska allows agencies to charge a fee for electronic services and products to recover actual costs, including a "reasonable portion" of development and maintenance. However, no-cost access public access must be provided to the same data via a public terminal. The work of the Public Information Access Policy Task Force resulted in amendments to Washington State statute to require various agencies to consider cost and other barriers to public access in designing their electronic information systems, and to keep the information as accessible as possible. This legislation also directs agencies not to "offer customized electronic-access services as the primary way of responding to requests or as a primary source of revenue."[15] In the interests of public access, Florida recently changed a mandatory electronic-transaction charge to a discretionary one. Minnesota's Government Data Practices Act has been amended in recent years to allow a "reasonable fee," based on actual development costs, for government databases and software which are commercially valuable and were developed with public funds. Indiana provides most of its electronic applications free of charge to residents and businesses, but "dynamic" applications (i.e., ones needing frequent updating) are available only to fee-paying subscribers. Georgia passed a law in 1993 that allows charging for electronic access to most public information; these charges are not limited to recovering costs.

Fees for electronic access can be controversial. In Nebraska, the state legislature intervened in a contract between an agency and a private firm to offer fee-based electronic access in a program that began as a free pilot service. In at least one state, Louisiana, the attorney general has issued an opinion that fees for copies should reflect only the expense of generating the information, not its commercial value.

However, a growing trend among states is to get into the business of fee-based public information services, typically through a public corporation such as New Mexico's TechNet, or through a contract with a private firm such as Nebrask@ Online and Access Indiana. The relative merits of such models are detailed in Chapter 5 below as part of a larger discussion of cost recovery. In Geor-

[15] Chapter 171, Laws of 1996.

gia, it has been clarified after some concern arose that the state's GeorgiaNet service cannot sell records per se, but only enhanced access to records. In most cases, these entities provide a mixture of fee-based enhanced services and free (or nominal cost) basic public information.

III. Privacy in the Context of Commercial Use of Electronic Public Records

Some states prohibit certain commercial uses of restricted public records containing personally identifiable information, when commercial use might intrude on the privacy of citizens. Washington State as well as New York, Rhode Island, Indiana and South Dakota have statutory provisions that refuse lists of names or other personal information if sought for a commercial purpose.[16] Kansas requires information requesters to agree not to use personal information from public records to conduct direct-sales marketing. Georgia briefly prohibited all commercial use of public records with a law passed in 1992 and repealed the following year.[17] California amended its public records law in 1994 to exempt voters' home addresses, phone numbers and occupations from release to the public, although journalists and researchers can still access this information. This approach has some momentum on the federal level as well. The federal Drivers' Privacy Protection Act of 1994,[18] which takes effect in 1997, prohibits states from releasing personal information from drivers' registration databases to the general public, but permits access for certain uses to businesses.

Another approach to protecting citizens' privacy is a "fair information practices" policy that provides citizens the opportunity to review and correct any public record that contains personal information about them. Fair information practices laws can be quite comprehensive, embracing eight basic principles: openness, individual participation, limited collection, data quality, limited use, limited disclosure, security and accountability. The federal Privacy Act of 1974[19] provides a process for citizens to view records pertaining to them and to request amendment of inaccuracies. The Privacy Act also places restrictions on the use and disclosure of personal information (for example, information collected for one purpose may not be used for another without notifying and obtaining consent from the subject of the record), and requires federal agencies to keep records of the date, nature and purpose of certain disclosures of personal information. Congress has also considered legislation to establish a Privacy Commission for the purpose of studying information systems.

A number of states including Virginia, New York, Hawaii, and California have fair information practices laws. Washington State's public electronic access law contains several provisions for information practices and data protection: agencies are directed to ensure the accuracy of personal information to the extent possible, and to establish mechanisms for citizens to review and request correction to information about them contained in public records.[20] Wisconsin created and subsequently abolished a Privacy Council and a Privacy Advocate to recommend state and local privacy protection policies.[21] In their place, a more narrowly-focused Telecommunications Privacy Council was created by the 1995 Wisconsin Legislature to monitor citizen concerns and complaints on behalf of the state utilities and telecommunications commission. Oregon recently amended its public records law to provide a process for citizens to prevent disclosure of their home addresses and telephone numbers, if disclosure would endanger their or their families' personal safety.

[16] NCSL page 8.

[17] Joint Committee on Information Technology Resources (Florida), "Electronic Records Access: Problems and Issues" (January 1994). In 1992, Georgia amended its public records law to include the following language:

"No public officer or agency shall be required to provide access to public records which are to be used for commercial purposes. The requesting party shall sign a statement agreeing not to use information gathered pursuant to said request for commercial purposes. Commercial purposes shall not include news-gathering requests for information or legitimate research for educational, scientific, or public purposes." (Official Code of Georgia Annotated Section 50-18-70 as amended by Ga. L. 1993, p. 1436, Sec. 1 and 2).

According to staff in the Georgia Attorney General's Office, the 1992 amendments were intended to address a perceived loophole in statute, under which a publicly-owned architectural plan was requested successfully as a public record. GeorgiaNet, the public corporation created in 1990 to provide electronic access to public information on a revenue-generating basis, had concerns that its information systems could be similarly requested.

The blanket prohibition against commercial purposes was considered unworkable because of widespread opposition from a variety of business users and because of difficulties with implementation. A 1993 amendment deleted the 1992 language as well as language that prohibited release of information for "commercial solicitation." Currently, Georgia's public records law appears to be silent on the question of commercial use per se. Specific exemptions are provided, however, to prohibit release of certain proprietary information (related to research); computer programs and software "used or maintained in the course of operation of a public office or agency" specifically areexempted from the statutory definition of "public record."

[18] 18 U.S.C.A. Sec. 2721.

[19] 5 U.S.C.A. Sec. 552a.

[20] RCW 43.105.310.

[21] Joint Committee (Florida), page 139.

Legitimate Business Use

Chapter 3

Toward a Policy Framework for the Commercial Release of Electronic Public Records

The Work Group's Answer to Question 1 in its Charter

How, and under what circumstances, should public records in electronic format be released for business or commercial purposes?

I. Introduction

Under Washington State law, public records that are lists of individuals cannot be released for commercial purposes unless there is a specific statutory authorization to do so (RCW 42.17.260(9)). The 1996 Legislature introduced and passed two bills, HB 2790 and HB 2604, that would have further expanded the growing number of exemptions to this prohibition.

Together, the bills raised what Governor Mike Lowry viewed as "serious questions that state policy now fails to answer." On March 30, 1996, the Governor vetoed the bills and announced that he would convene a Work Group to review current state practices and policies related to the commercial release of public records.

The Governor expressed concern over the cumulative effect of hundreds of exemptions over 24 years — compounded by the impact of new digital technologies — on how government handles public records. "As state government responds to emerging technologies, it is likely that we will have to modify the way we control and disburse the information we hold."[22]

His instructions to the Work Group were clear: "The charter of the Work Group is to recommend whether and under what circumstances government records in electronic format should be released for commercial, profit-making purposes, with particular emphasis on safeguarding the privacy rights of individuals who are subject to those records."

At its first public meeting, the Governor told the Work Group that commercial access to public records represents a growing question in the electronic age. Indeed, public policy tends to lag behind societal developments. The lag is even more pronounced in dealing with electronic records because of relentless technological change. The rapid advances related to the Internet and other digital technologies often eclipse the public sector's ability to stay abreast of the technological developments and account for their social impact.

The Governor asked the Work Group to send the clearest possible message by developing a coherent statewide policy that balances legitimate business and government interests with personal privacy concerns.

This chapter reflects the direction of the Work Group as it creates the framework for a single, coherent, statewide policy on commercial release of public records. The group recognizes that the criteria for determining permissible commercial use of public records must be kept relatively simple. In the group's view, permissible use is measured against what is disclosable under the law and hinges on the question of public benefit.

II. The Public Benefit of Commercial Access to Government Electronic Records

The Legislature has found "that government information is a strategic resource and needs to be managed as such and that broad public access to non-restricted public information and records must be guaranteed."[23]

[22] HB 2604 (Full Veto).

[23] RCW 42.17.261 (1994).

Broad, legitimate and authorized public access clearly constitutes a public benefit. The Open Records Act was passed by citizen initiative in 1972 to codify those benefits — providing citizens with the information they need to hold government to account.[24] The Open Records Act is structured to favor access over privacy. Its mandate for open government is tempered only by a provision to evaluate those records whose release would be "highly offensive to a reasonable person and of no legitimate public concern."[25]

Commercial release involves a broad spectrum of public records — from legislative and regulatory information to personally identifiable information. The latter is allowed only through legislative exemption. The end result is a system that can treat the same information differently from agency to agency. Information that is prohibited from release under one government program is available from another. The inconsistency extends to the treatment of records between programs within agencies. For example, proprietary business information — the release of which can leave a company that complies with regulatory reporting requirements at a competitive disadvantage — is excluded from release under some statutes, but not all. As a result, information that is excluded from release at the Department of Revenue may be subject to release at a number of other agencies. Such agency-to-agency variance also effects personally identifiable information.

The patchwork quilt of release provisions — overlapping in some areas and threadbare in others — causes uncertainty and confusion for the agencies that are entrusted with the proper management of public records. If the trustees of public records are confused, it is understandable that individuals (the subjects of those records) are expressing growing concern about how information about them is handled. The uneven statutory provisions governing release of public records is complicated by issues related to technological change and commercial release.

Commercial Release

Commercial release itself cannot be treated as a monolith because the nature of commercial interests varies widely. Some private interests use public records to comply with regulatory or legal requirements. Others are full-service information resellers — such as Lexis-Nexis, TRW, and Commercial Information Systems (CIS).[26] These information resellers typically apply custom indexing and searching capabilities to a broad range of data, from both public and private sources.

In written and oral submissions to the Work Group, CIS and its clients advocated the identification of "permissible uses" and permitted users of public records in electronic form. Given the Work Group's charter, any discussion of permissible uses and users necessarily begins with the notion of public benefit. Again, the universe of records under discussion is defined by what is disclosable under the law, coupled with the subsequent exemptions.

As steward of public records, government is responsible for deriving benefit for citizens through the proper use of data. Public benefit is derived through direct governmental use of public records, as is the case when data is used by planners to deliver services more effectively or to anticipate future demands for infrastructure. Public benefit can also be derived through certain private-sector uses of public records. For example, there is a strong public safety interest in notifying vehicle owners of a recall in a timely fashion. The recall is done on behalf of a manufacturer by an information reseller using public records.

Government is often the holder of the unique and authoritative record to which all other records

[24] As is discussed in Chapter 5, commercial release may play a vital role in sustaining electronic public access systems.

[25] RCW 42.17.300.

[26] CIS actively supported the passage of HB 2790, one of the bills vetoed by the Governor in March 1996.

refer. To expand on the example given above, the Department of Licensing (DOL) holds the authoritative records on registered motor vehicles in the state. The use of DOL data by an information reseller to notify vehicle owners of a recall or safety defect has a demonstrable public benefit. The auto manufacturer, the information reseller working on its behalf, insurance companies, the government and the public all derive benefit from the initial release of those motor-vehicle records.

There are also clear (albeit different) public benefits derived from the commercial release of land title records for sellers, buyers, realtors and lenders. The records provide the legal underpinnings of significant economic transactions. All parties have an interest in verifying the status of property before and after its sale. Again, government holds the unique and authoritative records.

Public records are of considerable value in planning both public infrastructure and private enterprise. Demographic, labor market and import/export data are important in projecting the demand for daycare facilities, schools, retirement centers and transportation infrastructure. The data are also instrumental in siting decisions for manufacturing plants, housing developments and retail outlets.

Distinguishing Between Commercial and Business Use

Another category of use demonstrates the subtle but important distinction between commercial and business use.

The Open Records Act prohibits the release of lists of individuals for commercial purposes. In opinions by the Attorney General, commercial purposes are defined as "profit expecting activity." Under such a definition, a list of vintage car owners could be released to an antique car club but not to an auto dealer because the dealer has a profit expectation and the club does not.

Beyond the distinction between commercial interests and the not-for-profit sectors, there is a distinction to be made between commercial and business use of public records.

Many businesses rely on a second or third party to corroborate information given to them. Importantly, such verification is often needed to comply with government regulations. Hiring decisions provide a number of illustrative examples in this regard. Transportation companies must check on applicants' driving histories. Schools and daycares must ensure that applicants do not have criminal histories that would put children in harm's way. Employers are required to check an applicant's eligibility to work in the United States.

In all these cases, public records are used to verify certain information in order to conduct business in a legal and responsible manner. It follows, then, that government has a duty to release the information needed to comply with obligations it imposes on the private sector.

In contrast, public records are sometimes used for unsolicited business contact or other purposes where there is no demonstrable public good. Such commercial use, often done without the subject's knowledge or consent, includes securing lists for the purpose of direct mailing or the creation of personal dossiers or profiles through the compilation of data from once-discrete databases.

In any commercial release of public records there is likely to be a mixture of public and private benefit. In some instances, there is a predominant public benefit. In other cases the public benefit is incidental to a predominant private benefit. In still other cases the public and private benefits are balanced.

The place of any particular commercial or business use on the continuum between public and private benefit has important policy and planning implications. To the degree that commercial release lends itself to public benefit, those uses should be supported by the release of the needed information. As the pendulum swings the other way, in instances where any public benefit is only incidental to a predominantly private interest, the release of records should be restricted.

The planning issues follow from the broader policy concerns. As agencies face increased demands for services from the public while budget levels remain static (or shrink), the support of electronic-access systems must be justified in terms of public benefit.

Efficiency

A number of agencies, together with the Washington Association of County Officials and the Association of Washington Cities, told the Work Group that records requests are growing rapidly as electronic records become the norm. Agencies report that servicing requests often divert resources away from the agency's legislatively mandated mission. The departments of Licensing and Health have expressed particular concern that any framework for commercial release factor in the cost implications of producing the records in such a way that comports with state law and is usable to an external party. Such concerns are not always reflected in discussions of greater government efficiencies through the use of technology.

Proponents of HB 2790 said its provisions would give government more powerful and user-friendly capabilities in manipulating electronic public records. Under the bill, a private-sector interest would add value to those records and provide government with access to the improved data.

As envisioned, private-sector participation would allow government greater access to state-of-the-art technology and the ability to better manage its data. Private-sector participation would also help mitigate the technology-related risks and costs. To be clear, such partnerships are not necessarily inconsistent with the proper stewardship of sensitive information with which government has been trusted.

The use of private-sector consultants and contractors to improve data or enhance systems to better manage data is an everyday (and long-established) practice by state agencies. That data and system improvements can be done legally without any additional legislative authorization raised questions, in the view of the Work Group, about the implementation of HB 2790.

It is unclear how HB 2790 impacts the ownership of, and control over, public records. So long as the records remain a public trust (as they now do under agreements with private vendors), government has the authority to prescribe permissible and non-permissible uses. If the rights to those records were to be transferred as part of any value-added arrangement, the government (as the public's trustee) would lose any right to control use by second or third parties. Its ability to curb abuse would likewise be lost.

By itself, efficiency may be an inadequate test for justifying the commercial release of public records. However, efficiency should be included in a broader test of public benefit.

III. Stewardship of Public Records

One of the othe challenges faced by the Work Group was how to deal with secondary use — and in some cases, abuse — of public records even when their initial release is justified by the public benefit test.

As discussed above, the categories of acceptable use include:

- information to hold government accountable;
- information to comply with government regulations;
- information to support public-sector decision-making; and
- information needed to deliver services on behalf of government.

Government agencies are responsible to three "publics": (1) the taxpayers of Washington state, (2) the millions of people served by agencies, and (3) the entities with which some state agencies contract to provide services to citizens on their behalf. Each "public" has a different need for information — and often a different expectation about how the information will be handled. The degree to which those expectations differ often only becomes clear after the fact.

An example from health care may help illustrate what is in practice a "stair-stepped" approach to handling certain sets of sensitive data. A health-care provider needs a certain detail of information to treat a patient. An insurance company will need some information about the treatment in order to pay the claim. An employer may need to verify that a treatment has taken place to ensure that the patient is eligible for sick leave. The citizen — who is simultaneously the patient, claimant, employee and taxpayer in this scenario — has a legitimate expectation that her records will be kept confidential except to satisfy the specific needs of the other parties. Currently, state law limits the dissemination of health-care information without the patient's consent.[27]

Original Orbit

Public benefit eludes easy definition. A useful model for delineating among potential uses based on their public benefit was introduced by a Work Group member. Under this model, the highest public benefit is realized when the records are used within the orbit for which they were collected. For example, the highest public benefit from health records is when they are used within their original orbit — that is, the delivery and planning of health services. The vehicle recall example used above would also fit within the original orbit of motor vehicles records because it represents an extension of the public safety role performed by the Department of Licensing. Original orbit as used here is not synonomous with original purpose. Original orbit recognizes that there are legitimate uses that are consistent with and, in fact, further a public mission and serve as an extension of original purpose.

However, the subsequent use of those motor-vehicle records for direct-mail campaigns or siting decisions for retail outlets would be outside the original orbit. The use of public records which goes beyond the original orbit raises questions of secondary use which, as stewards of the records, government must address.

Secondary Use

There is no consistent policy governing secondary use of public records under statute. As demonstrated by the Work Group survey of state agencies summarized above, practices by state agencies and local governments vary widely. Once released, the subsequent use and disposal of public records with personally identifiable information (and the prospect of secondary use) is a matter of growing public concern. Depending on the jurisdiction and the precise nature of the information, its disposal after initial release may be a matter

[27] Chap 70.02 RCW.

covered by statute, regulation, contract or left to the vagaries of the marketplace.

The importance of, and public concern over, secondary use of electronic public records has been underscored repeatedly during the Work Group's brief tenure. The steady diet of news reports about such use is summarized below in the discussion of safeguarding personally identifiable information. The revelations have raised serious questions about how much information is considered "public." Importantly, the rules (and the law) have not changed — the technology has. Indeed, digitization has forced these issues onto the table. The digital environment destroys the inherent protection afforded to people in an earlier analog era — gone are the cumbersome paper-based systems that made it difficult to get at and manipulate personal information.

Misuse and Abuse

A member of the Work Group portrayed the misuse of digitized personal data in graphic terms — referring to it as "high-tech assault." In the Group's view, there is no interest in creating a new bureaucracy to handle data. In its view, it is more efficient to deal with abuse using sanctions after the fact. Ironically, the only sanctions in the Open Records Act are against failure to release. There are no enforcement provisions under the Act to mitigate against abuse related to improper release or subsequent misuse of lists of individuals.

Review of Existing Law

The public records laws are not administered by any agency. Generally, amendments to the law are suggested by agencies, the media and business interests that have recognized problems unique to certain governmental records. There has been little overall policy development, with the result that the law resembles a patchwork quilt. This is true with commercial access to government records.

The law only contains one provision generally applicable to commercial access to any public record. The original language is essentially unchanged and is found at RCW 42.17.260(9):

> "This chapter shall not be construed as giving authority to any agency, ... to give, sell or provide access to lists of individuals requested for commercial purposes, and agencies, ... shall not do so unless specifically authorized or directed by law: PROVIDED, HOWEVER, That lists of applicants for professional licenses and of professional licensees shall be made available to those professional associations or educational organizations recognized by their professional licensing or examination board, upon payment of a reasonable charge therefor ... ."

There are no reported judicial decisions regarding its meaning. Its interpretation has been the subject of several Attorney General opinions, however. While those opinions are not absolutely consistent, they can be summarized:

- the statute only applies to lists generated by the agency, not the "raw data" containing the original information,
- of natural persons, not business entities,
- when the information is requested by a profit-expecting entity,
- for the purpose of contacting the people on the list in order to further that profit-expecting activity.

For example, title insurance companies routinely access property information from county assessors (sometimes on-line) that contain real property information, such as ownership, sales, etc.[28] That is permitted because they do not contact the people on the list. An association of antique car owners can contact those owning older vehicles because it was not a profit expecting ac-

[28] AGO 1980 No. 1.

tivity.[29] The statute does not contain any penalties for inappropriate use of the records.

Some categories of public records have been accessible by only some requesters. For instance, driving abstracts are available to some commercial entities. The abstract includes accidents in which the person was driving, any reported convictions, forfeitures of bail and the status of the person's driving privilege in this state. Under RCW 46.52.130, the abstract

> "...shall be furnished only to the individual named in the abstract, an employer, the insurance carrier that has insurance in effect covering the employer or a prospective employer, the insurance carrier that has insurance in effect covering the named individual, the insurance carrier to which the named individual has applied, an alcohol/drug assessment or treatment agency approved by the department of social and health services, to which the named individual has applied or been assigned for evaluation or treatment, or city and county prosecuting attorneys. ..." (Emphasis supplied)

The abstract is to be used only for related business purposes and a violation is a gross misdemeanor. It should be noted that the information in the abstract is generally a matter of record in courthouses in each county. The records are generally accessible by anyone. The legislature has treated the cumulative, electronic database of the records differently, apparently out of concern that this information could be misused when collected in a single place.

Criminal history information (Chapter 10.97 RCW) reflects an individual's contacts with the criminal justice system, convictions, arrests, etc. That is also generally available to the public in the county where the contact occurred. Anyone can obtain records of conviction about anyone, from the database which collects that information and is maintained by the State Patrol.[30] Curiously, the Legislature has provided that prospective employers whose employees will be in contact with children or vulnerable adults may obtain only those conviction records relating to physical or sexual abuse.[31]

Similarly, accident records maintained by the State Patrol are available to "interested parties," meaning the representatives of the parties to the accident, including insurance companies.[32] These records are otherwise declared to be "confidential" and may not be introduced as evidence in court. Failure to file an accident report is a gross misdemeanor and can result in a suspension of a driver's license.[33] However, there is no penalty for the inappropriate use of the records by any of the "interested parties."

Possible Disincentives

It is not unusual to find criminal penalties attached to statutory violations; however, given the workloads in every prosecutor's office, it is unlikely that anyone has ever been charged, much less convicted for the wrongful use of a public record. It is more likely that a financial penalty enforceable by agencies or aggrieved citizens would discourage violations. Since the perceived threat is the collection of information on individuals, the penalty could be assessed at a fixed amount for each name in the database together with the recovery of court costs, including attorney's fees.

Of course, penalties only have meaning if there is a significant chance of detection. Given the widespread availability of information about individuals, there should be a mechanism that permits detection of the misuse of governmental records. The Federal Election Commission (FEC) is authorized to allow the "salting" of the lists of contributors by political committees to prevent solicitation of those contributors by other political committees. The lists can contain pseudonyms with ad-

[29] AGO 1975 No. 15.

[30] See, RCW 10.97.050(1).

[31] See, RCW 43.43.830.

[32] See RCW 46.52.080.

[33] See RCW 46.52.020, .030.

dresses which allows detection of solicitations by unauthorized committees. In the Work Group's view, agencies should be permitted to "salt" their lists to detect unauthorized use.

The problem here extends beyond the Open Records Act's silence on providing disincentives to the abuse of public records. A change in the underlying technology that holds and manages records is challenging the assumptions that have been embedded in our print-based culture since Gutenberg.

IV. Digital Records: Decomposition of the Document

The Open Records Act does not make a distinction between paper-based records and those in electronic form. Why would it? A quarter-century after its passage, the impact of digitization is only now being understood by industry, government and individuals. The founder of the Media Lab at the Massachusetts Institute of Technology, Nicholas Negroponte, contends that digitization is not just a technological change — it is a societal transformation. To apply Negroponte's language to the present case, public records are being transformed from "atoms" (paper) to "bits" (electronic). Digital technology fundamentally changes the nature of records. The change is rooted in the fact that "bits commingle effortlessly."[34] That fact brings with it considerable promise — and the risk of dangerous pitfalls — to the proper stewardship of public records.

In the shift from paper-based to electronic records, there has been the loss of the contextual. People may still fill out forms in conducting transactions with government. However, that paper record begins to decompose the instant that discrete pieces of information from a single document become data elements in a data base. In fact, the paper form as a container of data has largely been replaced as the "unique copy" of the record by a series of digital fields. Because "bits commingle effortlessly," any combination of data elements can be manipulated in ways that improve efficiencies in service design and delivery but may not fully be understood by the subjects of the original record.

While information provided on a paper form will remain static over time, the digital environment is dynamic. Data elements in electronic form can be updated, changed or corrupted over time. Whereas a paper record is a paper record, elements of an electronic record can be reconfigured and commingled endlessly. Public policy that is based on the assumption that records are pieces of paper in a filing cabinet risks missing the dynamic of the digital age. The malleability of electronic data raises questions related to the temporal elements of public records: version and transaction control. These issues tend to escape widespread attention — with the possible exception of the IT community — but raise significant stewardship concerns at the public policy level.

V. Software Development and Public-Private Partnerships

This chapter has already made a number of important distinctions: public vs. commercial access; commercial vs. not-for-profit use; commercial vs. business use; public vs. private benefit; and, analog vs. digital records. Within the realm of digital records, it is necessary to make at least one additional distinction — between the electronic records and the software that creates them.

Digital records do not exist in a vacuum. They are created, maintained, safeguarded, manipulated and updated by computer software. The software

[34] Nicholas Negroponte, *Being Digital*, New York, Albert A. Knoff, 1995:18.

represents a significant public investment. The software is made up of millions of lines of code that create virtual containers for the data — and whose design sets out the relationships of data within and among those containers. The codification of those relationships in software is an increasingly complex and risky business.

To gain access to state-of-the-art software-development expertise, state agencies have an established practice of contracting with private-sector firms. There are no prohibitions against public entities using private contractors to add value directly or indirectly (the latter through building or enhancing government IT systems to better manage data).

Done properly, such arrangements can produce more advanced systems at less cost to taxpayers. To further contain costs, the relationship between public agencies and vendors can be cast in terms of a public-private partnership. Under such partnerships, risks and rewards are shared with the private contractor. While the records themselves remain a public trust, the ownership of the software developed to manage them should be a matter of negotiation. In some cases, the software may become the exclusive property of the agency. In other cases, it may be jointly owned by the state and the private partner. In all cases, there should be provisions ensuring that the software is available for legitimate governmental use including public inspection of records where specified in statute.

Under joint ownership, the state has guaranteed access to the software needed to manage its data. For its part, the private partner is able to leverage the research and development costs it absorbed on a given state project by applying all or part of the code on other projects with other customers.

A survey by the National Association of State Legislators reports that 20 states have exempted software from their open records legislation. Some parties are concerned that a software exemption may limit the public's access to its records. In the Work Group's view, this concern can be addressed through contractual provisions that ensure that the state (as trustee) will have full and perpetual access to the jointly owned software for governmental use — including public access.[35]

A software exemption would allow the state to protect the public investment in proprietary software, leverage its resources through public-private partnerships and other such strategic alliances, and ensure that the software which supports public records can be maintained, enhanced and refurbished as necessary.

VI. Summary

In answering the question, *How, and under what circumstances, should public records in electronic format be released for business or commercial purposes?*, the Work Group finds:

- digital technology changes the nature of public records themselves, bringing with it the prospect for greater governmental efficiencies and the need for additional safeguards to protect personally identifiable information.
- many companies rely on a third party to corroborate information given to them by applicants and customers in the legitimate conduct of their business.
- such verification is often needed to comply with government regulations.
- government records are used to verify certain information in order to conduct business in a legal and responsible manner.

[35] Such a public access provision would ensure that the software necessary to read the data would be available for the examination of records while protecting the public investment in the software itself.

- the universe of public records subject to disclosure is defined by statute.
- public records are a public trust. The ownership of those records should not be transferred to other parties.
- the highest public benefit from public records is when they are used to further a public mission. The public-benefit test of remaining within their "original orbit" — that is, use that advances an agency's public mission — is true for legitimate governmental or business uses of information.
- government has a duty to release the information needed to comply with obligations it imposes on the private sector.
- permissible business use should meet a test of demonstrable public benefit.
- the use of government records for "legitimate business purposes" needs to be distinguished from "commercial purposes" as used in the Open Records Act.
- current restrictions on "commercial use" — defined by the Attorney General as direct contact for profit-making purposes — should be maintained.
- the Open Records Act is silent on sanctions against improper initial release of public records — and on misuse related to secondary use.
- the Open Records Act does not distinguish between public records and the software that creates and maintains them in a digital environment. In the absence of any protections for the significant public investment in proprietary software, the state faces difficulties in ensuring the future availability, enhancement and refurbishment of these systems.

Safeguarding Personal Information

Chapter 4

Meeting the Individual's Expectation of Privacy by Containing Records Within Their Original Orbit

The Work Group's Answer to Question 2 in its Charter

How can citizens be assured that personal information about them will be safeguarded when public records in electronic format are released for business or commercial purposes?

I. Introduction: The Privacy Landscape

The digitization of records containing personally identifiable information has compounded some long-standing privacy concerns and, in some cases, created new ones. Since the Governor announced the creation of this Work Group on March 30, 1996, there have been more than 100 news stories about the impact of digital technology on the use and abuse of personally identifiable information.

It is important to note that there are safeguards in Washington State that would prevent a repetition of the most infamous cases from other jurisdictions. The Open Records Act places relatively few restrictions on private disclosure but it does, importantly, exempt from disclosure 33 categories of government documents, including personally identifiable information in files of public school students, hospital patients, welfare recipients, public-agency employees and appointed or elected officials.[36]

The summary of news stories that follows is not intended to frighten or evoke an alarmist response. Rather, it is intended to demonstrate that both the public and private sectors are struggling to deal with the impacts of technological change (coupled with human misconduct) on records management.

The relative threats to personally identifiable information by the public and private sectors become clearer when their respective breaches are seen in juxtaposition. The activities of the private sector — with its ubiquitous "dataveillance" of consumers — would appear to have a greater long-term impact on the privacy of individuals than anything that government is doing by itself.

The summary that follows also illustrates the range of responses from other jurisdictions and the private sector which may be instructive in developing policies in Washington State. Some of the stories capture changing public attitudes and expectations about privacy — both those that see its erosion as inevitable and those that are taking measures to shore up safeguards. Finally, these stories are illustrative of the revelations that are fueling concern among citizens and with which public policy makers must deal:

• SOFTWARE GLITCH EXPOSES CREDIT CARD INFORMATION ON THE WEB: Credit card information submitted electronically by some shoppers on the World Wide Web was accessible by anyone using a simple Web browser. Software for conducting electronic transactions called SoftCart was improperly installed by an undisclosed number of merchants. As a result, completed order forms containing credit-card information and other personally identifiable information were not placed in special directories that are not accessible to Web browsers.[37]

• TAPE RECORDING CALLS: The Washington State Patrol has suspended what had become a routine practice of recording private telephone conversations made from certain rooms at its Parkland, Wa., headquarters. According to published reports State Patrol Captain John Baptiste said the digital recordings constituted "a technical violation that did no harm." He said it was an innocent error made in the interest of improving efficiency. Calls were recorded for over a year with-

[36] RCW 42.17.251 (1994).

[37] *Wall Street Journal*, November 8, 1996: B6.

out any notice telling callers their phone conversations were being recorded.[38] The Washington State Privacy Act restricts the recording of private conversations, making it unlawful to make recordings without first obtaining the consent of all parties to the communication.

• PERSONAL USE OF AIDS/HIV DATABASE: A computer database of nearly 4,000 AIDS- and HIV-infected individuals was allegedly used by a Florida man to look up the names of potential dates for himself and his friends. Called "the nation's largest ever security breach of AIDS information," the case "has thrown a spotlight on new threats to medical confidentiality as computer networks, insurance databases and hackers pry out the most intimate details of people's lives." Copies of the list of individuals were sent to the man's employer — the state department of health — and two area newspapers. Officials are investigating whether the list may have been published on the Internet or whether there is a network of AIDS information brokers.[39]

• SURF TRACKING: The 1996 Equifax/Harris Consumer Privacy Survey for the Internet illustrated the changes in perceptions that come with using a new technology. Seventy-one percent of Internet users believed the tracking of their activities on the Internet was intrusive, compared to 63 percent of non-users. Sixty percent of users said their anonymity should not be compromised when they visit a Web site or use e-mail. Only 45 percent of non-users "were sympathetic to the desire for on-line anonymity."[40]

• INTERNET PRIVACY PROTECTION: An Internet privacy protection bill has been introduced in Congress, the latest in a series of legislative measures at the federal level to slow the flow of personally identifiable information.[41] Key provisions of the proposed federal Health Information Privacy Protection Act are intended to curb the growing trade in medical records.[42] Other initiatives included proposed regulations for the use of so-called smart cards over networks[43] and the introduction of (hotly contested) encryption standards.[44] In addition, the Attorney General has proposed new measures to prevent acts of on-line terrorism.[45]

• E-MAIL, VOICE MAIL AND PERSONAL AGENTS: The proliferation of e-mail and voice mail in the private sector has raised concerns over employer liability and personal privacy.[46] Recent anecdotal reports are often cast against the backdrop of a 1993 study published by MacWorld magazine. It found that 30 percent of employers in the survey were searching the computer files kept by employees. Knowing they were being watched, employees reported increased boredom, tension, anxiety, depression, anger and fatigue. The introduction of personalized search agents on the Internet, which track the on-line habits of individuals to identify their interests, raises the prospect that the cache gathered about individuals might be used (and abused) by others.[47] To address the privacy concerns raised by this technology, electronic agent services have turned to independent auditors to ensure personally identifiable information is not intercepted or released to third parties.[48]

• LEXIS-NEXIS P-TRACK CONTROVERSY: The respected information research service and reseller Lexis-Nexis was the focus of a national controversy soon after it launched a new service called the P-TRACK Personal Locator file in June. The company's promotional material initially said the service "provides up to three addresses, as well as aliases, maiden names, and Social Security numbers" and puts "300 million names right at your fingertips." Fueled by media coverage and Internet message traffic, Lexis-Nexis was flooded with complaints about the potential for fraud or other abuse.[49] Eleven days after P-TRACK launched, Lexis-Nexis removed the Social Security numbers

[38] John Gillis, "State Patrol admits it violated law," *Tacoma News Tribune*, Friday, October 18, 1996: A1, A10.

[39] "Aids list breach highlights confidentiality issues," *Reuters*, October 13, 1996.

[40] *BNA Daily Report for Executives*, October 10, 1996: A24.

[41] "Internet Privacy rules proposed," *Telecommunications Alert*, June 5, 1996, Vol. 13, No. 109.

[42] "Prepared statement by Steven Kenny Hoge M.D., Division of Government Relations, American Psychiatric Association, on the Health Information Privacy Protection Act [Discussion Draft] before the House Government Reform and Oversight Committee Subcommittee on Government Management, Information and Technology," *Federal News Service*, June 14, 1996.

[43] "Wait on smart card regulation, FDIC told," *The Regulatory Compliance Watch*, September 23, 1996.

[44] *Software Law Bulletin*, May, 1996: 77.

[45] Art Kramer, "Attorney General hopes to thwart online terrorists," *Atlanta Journal and Constitution*, June 6, 1996.

[46] "E-Mail and Voice Mail: Liability waiting to happen?" *Idaho Employment Law Letter*, July 1996, Volume 1, Issue 4; Robert Gellman, "On Privacy: The Question Industry doesn't want to answer," *DM News*, June 17, 1996: 44; and "Insurers, Corporations uncertain about need for on-line coverage," *Treasury Manager's Report*, August 30, 1996, No. 18, Vol. 4.

[47] "An intelligent agent is simply a computer program endowed with enough smarts to act as your personal assistant. In theory, an intelligent agent can act as your secretary, reference librarian, or stockbroker. It's designed to roam the Internet in search of just the information, sounds, or pictures you want. " See "Agents work for you," NetGuide Magazine, July 1, 1996.

[48] Rose Aguilar, "Privacy audit can keep secret," *Reuters*, August 6, 1996, 1:30 p.m. PT.

[49] Tom Abate and Erin McCormick, "When technology threatens privacy: Public anger grows as data providers sell our names, numbers and address," *The San Francisco Examiner*, September 20, 1996: A1.

from the service and provided a mechanism for removing names from the database upon request.[50] In its defense, a company spokesperson said, "There are a lot of people that don't understand how information is collected by any number of agencies. We are not the only company that purchases this type of database."[51]

• FTC SAFEGUARDS: In response to the complaints over P-TRACK, the Federal Trade Commission (FTC) urged Congress to tighten controls on commercial services that provide personally identifiable information about individuals for a fee.[52]

• INDUSTRY PRIVACY PRINCIPLES FOR THE INTERNET: A consortium of companies involved in electronic commerce via the Internet announced plans to develop a set of privacy principles for doing business over the global network. The Privacy Assured group came together in the wake of the Lexis-Nexis P-Track controversy. According to published reports, "Privacy Assured, which is a pilot program of the Electronic Frontier Foundation's eTrust project, will post its blue PA logo on Web sites that adhere to its standards." The proposed standards would prohibit member companies from knowingly listing information about individuals that has not been volunteered for publication. The eTrust program would disallow reverse searches to determine individuals' names from e-mail addresses, phone numbers or other information. Companies adhering to the standard would only release aggregated usage statistics, not individual information; and give individuals the option to remove their personal information from lists.[53]

• "KIDS OFF LISTS" PROVISIONS: The federal Children's Privacy Protection and Parental Empowerment Act put in place restrictions on on-line solicitation of children with a view to keep information about them out of the hands of sexual predators.[54] As part of a conference on Internet privacy, the FTC examined on-line marketing to children — including the collection and sale of information about their online behavior.[55] The Direct Marketing Association responded with a preliminary set of privacy guidelines for self-regulation. The proposal, if approved, would require marketers to post a privacy policy in an "easy-to-find, easy-to-read statement" that tells users how the information will be used.[56]

• QUESTIONABLE DATA USE AND INTEGRITY: A long-time information reseller is reconsidering its business model following a controversy over the use of automated mail information by a subsidiary.[57] Other recent stories have focused on data integrity and concerns about the accuracy of credit information. Some of these stories use as their benchmark a 1991 review of personally identifiable information held by the major national credit-reporting agencies. It found errors in 48 percent of records checked in 1991, an increase of 5 percent since a similar review in 1988.

• OREGON DMV RECORDS ON THE 'NET: Oregon Governor John Kitzhaber will ask the 1997 Oregon Legislature to redress the balance between privacy and public disclosure in the wake of a controversy over the publishing of the state's DMV records on the Internet. A Portland-based computer enthusiast, Aaron Nabil, purchased the Oregon DMV database for $222 and posted it on the World Wide Web.[58] The controversial Web site was suspended after Nabil and the state Department of Transportation were inundated with complaints from angry drivers "who mistakenly thought the records were private."[59] There are safeguards against such use in Washington State.

• PRIVACY CONCERNS OVER ON-LINE REGISTRIES: There has been a proliferation of new on-line registries that automate routine information handling, including on on-line registries of voters,[60] motor vehicles,[61] workers compensation

[50] Thomas E. Weber, "Lexis-Nexis Database Sparks Outcry on the Internet about Privacy Issues," *Wall Street Journal*, Sept. 19, 1996.

[51] Janet Kornblum, "Private lives online," *c|net news.com*, October 11, 4 p.m. PT.

[52] "FTC comes along on privacy," *Reuters*, September 23, 1996, 6:45 p.m. PT.

[53] *Broadcasting & Cable*, October 7, 1996: 87.

[54] "Prepared Testimony of Marc Rotenberg, Director, Electronic Privacy Information Center before the House Committee on the Judiciary Subcommittee on Crime on the Children's Privacy Protection and Parental Empowerment Act, H.R. 3508," *Federal News Service*, September 12, 1996.

[55] Denise Shelton, "Children-targeted marketing under fire," *c|net news.com*, May 14, 1996, 2 p.m. PT.

[56] Jim Davis, "Rules issued for online privacy," *c|net news.com*, June 4, 1996, 1 p.m. PT.

[57] Nancy Millman, "Questionable data sale to hinder Metromail IPO? R.R. Donnelley says unit no longer fits in," *Chicago Tribune*, June 4, 1996: 1.

[58] William McCall, "Vehicle files on Internet draws anger," *Tacoma News Tribune*, Aug. 8, 1996. The Oregon case is not, strictly speaking, an example of commercial use because the provider is not charging for access. There are other such services — such as Internet DMV — that provides on line searching of a number of state databases for $20 to $35 per search.

[59] Anthony Lazarus and Mike Ricciuti, "DMV data drives protest," *Reuters*, August 8, 1996, 11:45 PT.

[60] "Voters' register mustn't be an invasion of privacy," The Financial Post, August 22, 1996: 10.

[61] Janet Kornblum, "Web has fast lane to DMV," *Reuters*, August 6, 1996, 5:30 p.m. PT.

registry and drug registry,[62] as well as ones developed on behalf of the Social Security Administration and the Internal Revenue Service. The Social Security Administration is planning a pilot program to provide sensitive personal earnings information on-line.[63] The Internal Revenue Service (IRS) has suspended the development of Cyberfile, a service that would allow taxpayers to file their tax returns via the Internet, after a critical report that concluded the software used in the project was "undisciplined" and lacked adequate security requirements.[64] For its part, the U.S. State Department is distributing passport forms on-line but will not accept on-line registrations until network security and other technical issues are overcome.[65] Security concerns raised by these new registries and services parallel some of the perils of on-line shopping[66] and have also been linked to fears about e-mail disclosure.[67] Some of the new applications, which are collecting large amounts of personally identifiable information, have also brought with them concerns about how new sources of data will be used.

• FBI "FILEGATE" AND CREDIT STING: There have been allegations of abuse of personally identifiable information by public officials, calling into question the trustworthiness of the public caretakers in these cases. In August, credit card holders reacted angrily when they learned that federal law enforcement officials had used their credit information without their consent as bait in a sting operation.[68] News of the sting came on the heels of the revelation that White House staff allegedly accessed the FBI files of hundreds of citizens who worked for the prior administration.[69]

• DISCLOSING PERSONAL INFORMATION FOR THE PUBLIC GOOD: There are cases when disclosing personally identifiable information may result in public benefit but the criteria for release varies widely. For example, the Health Professions Quality Assurance Division at the Washington State Department of Health regulates the practice of health professions and enforces health and safety laws that protect the public from negligent, incompetent, or illegal health care practices. The names and registration numbers of those health care professionals facing disciplinary action are published as a news release and posted on the Internet.[70] In its survey response, the Department of Health told the Work Group it would like this service reduced in scope to disclose the names of only those health care providers that have been found guilty of charges against them.

• PRIVACY RIGHTS OF CONVICTED CRIMINALS: By contrast, the privacy rights related to the medical records of two criminals — one a convicted murderer and the other a convicted sex offender — were upheld despite challenges by The Seattle Times. "Privacy is a hot-button word, one that people — even criminals — increasingly cite in wanting to control what is known about them..." wrote Times executive editor Michael R. Fancher in arguing that "the public has a higher right to information about such people and about how are institutions treat them."[71]

One commentator wrote of the fundamental change in the way electronic information is collected, manipulated and distributed, "Everything from our taxes, health care, work, travel and military records to past scrapes with police or even sexual escapades — somewhere the information is only a few keystrokes away. The possibility for abuse is breathtakingly large — and growing."[72] The public response has been swift, sure, sometimes fearful, and sometimes angry. That citizen focus is vitally important in considering commercial access in general — and the privacy question in particular.

[62] John Deverell, "Drug registry sparks fears for privacy: Few rules yet on how new cache of data may be used," *The Toronto Star*, September 17, 1996: B1.

[63] Janet Kornblum, "Social Security sends info online," *Reuters*, September 27, 1996, 12:30 p.m., PT.

[64] Rose Anguilar, "IRS back to drawing board," *Reuters*, August 30, 1996, 1 p.m. PT.

[65] Janet Kornblum, "Your pass overseas, now online," *Reuters*, September 19, 1996, 1 p.m.

[66] Ilene Knable Gotts and Rebecca R. Fry, "Danger may await Internet shoppers," *The National Law Journal*, March 25, 1996: C9.

[67] Jim Dillon, "Digital Dialogue: Lexis-Nexis incident reveals e-mail disclosure fears," *The Dayton Daily News*, September 23, 1996: 15.

[68] Jim Newton, "Credit-card holders cry foul that accounts used in sting," *The Seattle Times*, August 30, 1996.

[69] Howard M. Shapiro, "Prepared Report of the FBI General Counsel on the Dissemination of FBI File information to the White House," *Federal News Service*, June 14, 1996.

[70] See the relevant page on the DOH web site at http://www.doh.wa.gov/Publicat/96-78.html.

[71] Michael R. Fancher, "Two criminals' privacy protected by state courts — and the public loses," *The Seattle Times*, Sunday, October 13, 1996: A27.

[72] David Gergen, "Our most valued right," *U.S. News & World Report*, June 24, 1996: 72.

II. Public Concern over Privacy in the Digital Age

Over time, as some have argued, the cumulative effect of such stories and the seemingly relentless advance of technology may lower expectations of privacy. In the near term, however, the opposite appears to be the case. Many of the developments described above have been met with mounting public concern. Individuals have reacted quickly and vehemently to revelations that what they had assumed was private information was available publicly from a growing number of sources.

In public comment, individuals repeatedly told the Work Group that government has greater access to information about people's lives than do private-sector interests. Government collects personal information on license applications, entitlements, hunting licenses and the like. Citizens are required to provide personally identifiable information as a pre-condition of receiving some services or benefits from government. Government is trusted with personal information and the writers' expectations are that personally identifiable information would be handled in a way that would not break that trust. One writer expressed it this way: "The citizenry of the great state of Washington highly values its trust and confidence in its public servants ... to properly and adequately protect the individual, personal, and private interest and safety, in all functions of society."

The Work Group respects the concerns expressed through the many thoughtful comments it received from members of the public on this important question. In fact, the overwhelming majority of comments from private citizens were concerned with privacy. In response to the revelations about the availability of personally identifiable information, writers called for additional protections on privacy. Some writers suggested that any privacy standards should be based on consent. Importantly, they wanted both to curb the amount of personally identifiable information in circulation in a networked world and to be notified that information about them was being gathered in the first place.

A number of writers expressed the fear that they could become victims of crime through the misuse of personally identifiable information. They expressed concerns about the prospect of credit or identity fraud and the risk of employment and insurance discrimination. The concerns extended to fear that personally identifiable information might be misused in cases of stalking and domestic violence. As one writer put it, "the simple fact is that there are a lot of us out here hiding from someone who wishes to do us harm."

In the view of many writers, computerization and digitization has brought with it the need for more safeguards and the need to "fight harder" to protect personally identifiable information. Some writers cited what they viewed as a lack of enforcement of existing laws and a lack of recourse in the case of violations. Still other writers questioned the necessity for the disclosure of personally identifiable information from government sources for secondary purposes, suggesting that there are alternative sources of information through consumer tracking and other private-sector initiatives.

Taken as a whole, public comment has tended to revolve around three policy and process questions:

- Who owns the unique copy of the record to which all others refer?
- What safeguards are in place to protect the integrity of the unique copy?

- What are the government's responsibilities related to secondary use of public records?

The majority report from the public is that there is an imbalance between technological advances and existing privacy protections.

III. Legislative Background

Public policy on privacy "seeks to balance business' and government's needs for access to information with the individual's expectations of privacy."[73] In the veto messages that created the Work Group, the Governor recognized that the group's deliberations "will bring into focus a complicated debate that will reveal conflicting values about public records, privacy, the future of technology, and government accountability."[74] Efforts to balance these competing values have resulted in both state legislation and citizen initiatives — the Open Records Act and the Washington State Privacy Act being the most prominent among them.

Privacy safeguards in Washington State statute includes a prohibition on the interception or recording of "private" communications by phone, telegraph, radio, "or other device" between two or more people without consent.[75] There are also statutory prohibitions on automatic dialing and announcing devices for solicitation purposes[76] and unsolicited fax messages.[77] The 1996 Legislature amended the Open Records Act to include provisions that address the accuracy, integrity and privacy of government records and information. It instructs state agencies to "establish procedures for correcting inaccurate information, including establishing mechanisms for individuals to review information about themselves and recommend changes in information they believe to be inaccurate."[78]

In creating the Work Group, the Governor affirmed that "Citizens' right to be secure in their private affairs and in their homes is essential to a free society. Washington State is very protective of people's right to privacy against governmental intrusions. The state constitution and Washington's Privacy Act afford greater protections than the federal Constitution and privacy laws...."[79]

For its part, the Open Records Act of 1972 — passed by a citizen initiative — provides broad access to government records to ensure the public's right to monitor government activities. "The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created."[80]

The Open Records Act also provides that "[t]his law shall not be construed as giving authority to any agency to give, sell or provide access to lists of individuals requested for commercial purposes, and agencies shall not do so unless specifically authorized or directed by law."[81] The Open Records Act also prohibits access to information "that is highly offensive to a reasonable person and of no legitimate public concern."[82] In addition, the Legislature and the courts have provided individualized protection for many categories of records regarding individuals, including health care, motor vehicles, taxes, arrests, Social Security numbers and the like.

In testimony before the Work Group, Dr. Ann Cavoukian,[83] co-author of the book *Who Knows: Safeguarding Your Privacy in a Networked World*, situated the Washington Open Record's Act in the larger context of access and privacy legislation around the United States and internationally.

Dr. Cavoukian expressed concern that the provision in Washington's Open Records Act to prohibit access to information "that is highly offensive to a reasonable person and of no legitimate public

[73] David W. Danner and Phil Moeller, *Telecommunications in Transition: Facilitating Advanced Communications Infrastructure in Washington*, Staff Report of the Washington State Senate Energy and Utilities Committee (February 1994).

[74] HB 2790 (Full Veto).

[75] RCW 9.73.030.

[76] RCW 80.36.400.

[77] RCW 80.36.540.

[78] RCW 43.105.310.

[78] ESHB 2406 (Full Veto).

[79] RCW 42.17.251.

[80] Initiative 276, Section 25 (5).

[81] RCW 42.17.255.

[82] Dr. Cavoukian is also the Assistant Commissioner of the Information and Privacy Commission of Ontario, Canada.

concern" is a very high threshold and may be "too high" if there is to be meaningful protection of personal privacy. When in doubt, agencies are most likely to err on the side of releasing information. Dr. Cavoukian asked the Work Group to consider the merits of a countervailing privacy provision that would require greater care in the decision to release personally identifiable information.

The Work Group has also heard from other parties who have made the argument that any such suggestion is "misguided." Michael J. Killeen is with the Communications and Media Law Department of the law firm of Davis Wright Tremaine in Seattle and legal counsel to *The Seattle Times*.[83] In a submission to the Work Group, Mr. Killeen wrote,

> Policy makers should recognize the risks in denying access based on overly broad concerns about personal privacy — risks that include loss of government accountability, an increased likelihood that official abuse will go undetected, less effective detection of dangers to public health or safety, and increased alienation of citizens from their government. The guiding presumption must be that if government has a reason to collect information about an individual, that information generally has an impact on the community, and therefore citizens are entitled to it.[85]

Mr. Killeen further wrote that "[p]olicies aimed at preventing misuse of public information should be formulated narrowly, in a way that does not unduly restrict access." In a story not directly related to the Work Group's activities, *Seattle Times* executive editor Michael R. Fancher recently told readers, "The *Times* has no interest in invading the private lives of ordinary citizens. Our interest is in maintaining the public's access to information about the performance of public institutions or about public policy."[86]

There may be common ground on this point. The Work Group has no interest in restricting access to information about the performance of public institutions or about public policy. The Work Group's interest is the government's duty to safeguard the private lives of ordinary citizens from invasion.

The Work Group notes with interest that the American Civil Liberties Union (ACLU) of Washington has begun an eighteen-month process to develop policies on commercial access to government records. In testimony before the group, ACLU-Washington legislative director Jerry Sheehan spoke of the organization's conflict on the issues related to commercial access. The ACLU historically has been a strong advocate of both access to government information and privacy. The present case is causing the organization to assess the two values in juxtaposition with a view to striking a balance between what appear to be competing interests.

That said, Dr. Cavoukian and other privacy advocates argue that openness in government and privacy protections for the individual are not competing but, rather, fundamentally compatible. She writes,

> [O]n one hand, the goal is to open the door and give people access to information, while on the other, the goal is to close the door and prevent outsiders from getting your information. But these two goals are seldom in conflict, for they apply to two entirely different types of information — one public, one not. Freedom of information applies to the public records of the government, records that are generally *nonpersonal* — that is, not about specific individuals. Privacy protection applies to a different set of records — *personal information*, associated with specific individuals. Public records *should* be accessible to the public; private records *should* be kept private, and used only for the purpose for which they were obtained.[87]

The director of the Washington, D.C.-based Electronic Privacy Information Center, Marc

[84] In his charge to the group, the Governor wrote, "the work group will not consider media access to government records in electronic format as a commercial use when such access is being requested for reporting purposes."

[85] Michael J. Killeen, "Electronic Records, the Public Disclosure Act, and Principles Governing Access," Presentation to the Governor's Work Group on Commercial Access to Electronic Records, July 11, 1996.

[86] Michael R. Fancher, "Two criminals' privacy protected by state courts — and the public loses," *The Seattle Times*, Sunday, October 13, 1996: A27.

[87] Ann Cavoukian and Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World*, New York: McGraw-Hill, 1996: 40-41. *(Emphasis in the original)*

Rotenberg, adds, "That there may be overlap between the public and the private does not diminish the essential importance of these principles."[88]

IV. Privacy: A Right in the Balance

The intersection of access and privacy is made even more difficult to navigate in the present case by rapid technological change and a historic problem with defining the concept of privacy.

In 1928, Justice Louis Brandeis called privacy the right "to be let alone" and "the right most valued by civilized men." Privacy is often defined negatively — that is, what it is not. For example, invasion of privacy is seen as interference with an individual's private affairs. Such an invasion can be warranted or unwarranted under law, depending on the purpose, the means employed and the nature of the information sought. There is no single, universally accepted definition of privacy. Nor are privacy protections specifically guaranteed by the U.S. Constitution, in contrast to freedom of speech, press, and religion, although the Supreme Court has recognized a Constitutional right of privacy. As detailed in Appendix C, each of the 50 states has had its own set of laws regarding privacy, creating unequal treatment of privacy from jurisdiction to jurisdiction.

The rise of electronic records and the underlying digital and network technologies have put privacy protections in play repeatedly over the years. Consider the chronology of one example from the federal government:

- The Privacy Act of 1974 was passed by Congress to protect the privacy rights of citizens from intrusions by the federal government. The act prohibited the inter-agency exchange of personally identifiable information held by government agencies.
- The Paperwork Reduction Act (1980) effectively allowed all personally identifiable information gathered by government to be made available to any agency. Coupled with the proliferation of automated technologies, the Act allowed "computer matching" across databases.
- The 1988 Computer Safeguards Bill was then introduced to again limit the federal government's use of computer records.[89]

As Dr. Cavoukian and her co-author suggest, privacy rights invariably must be balanced against other considerations — and those considerations may change over time:

> We do not suggest that privacy is an absolute right that reigns supreme over all rights. It does not. However, the case for privacy will depend on a number of factors that can influence the balance — the level of harm to the individual involved versus the needs of the public.[90]

Given that criteria, there would be a different balance struck for the release of personally identifiable information about a convicted sexual predator who has been released into a community than for a person in the same community who is HIV-positive. Protecting the identity of the predator may put children in harm's way. Disclosing the name of the HIV-positive individual may lead to loss of employment, benefits and housing.

Judging by public comment received by the Work Group and the media coverage of these issues, there is a growing concern that electronic records are both infinitely changeable and disturbingly durable. The public concern can be fairly summarized as follows:

- If you are alive, you are constantly creating records about yourself. That these records can be gathered, co-mingled and compared can

[88] Marc Rotenberg, "Privacy Protection," *Government Information Quarterly*, Vol. 11, No. 3, 1994: 254.

[89] Anne Branscomb, *Who Owns Information?: From Privacy to Public Access*, New York: 1994.

[90] Cavoukian and Tapscott: 16.

tell others more about you than you ever intended. Those records are also difficult to evade.

- Moving to a new town no longer affords the opportunity to re-create yourself. Before long, your employer, banker and local retailer probably have a pretty good idea of where you have been and what you have been doing. Depending on their resourcefulness, they can probably discover a skeleton or two — even if it has no bearing on your current life or relationship with them.

- That records can now follow you most everywhere points to the loss of "social forgiveness." Even minor misdeeds can follow otherwise solid citizens for life. In a networked world, there may be nowhere left to exercise your right "to be let alone."

V. Digital Records: Pendulum Swinging Back

In her testimony before the Work Group, Dr. Cavoukian commented on the impact of digital technology on personally identifiable information and the growing concern in the public about how information about individuals is handled in both the public and private sectors.

She said the recent Lexis-Nexis P-TRAK controversy was an illustrative example of "driftnet data fishing," highlighting the impact of digital technology on records stewardship. In a paper-based world, records were discrete and had to be compared and compiled by hand in a difficult and time-consuming process. However, the emerging digital environment lends itself to the ready co-mingling of once-discrete records.

Dr. Cavoukian said the short answer to the question before the Work Group was that one cannot provide absolute safeguards for personally identifiable information when public records are released for commercial purposes. However, the long answer was that there were a number of steps that can be taken — voluntary privacy codes, physical and computer security provisions, and the redaction of personally identifiable information — to provide some safeguards for citizens and their personal information. If those steps are taken, it is possible to re-introduce at least some level of "social forgiveness."

Before a decades-long automation process began in government, paper searches provided a form of protection because of the effort required to find the information. It was a cumbersome process that discouraged all but the most motivated requester. The gathering of personally identifiable information in searchable databases creates risks today that did not exist before. After years of focusing on the automation process, the pendulum appears to be swinging back to consider the combined effects of all such technological advances on personal privacy. It is not that the public is relaxing its demands on government for efficiency and responsive service delivery. More to the point is that the public expects the benefits of those efficiencies without compromising its personally identifiable information.

VI. Prospects for Self-Correction

The Work Group was asked by the Governor to address safeguards for personally identifiable information when public records are released for business or commercial purposes. As will be discussed below, there are measures that government can take to protect personal information provided by citizens.

Everyone exchanges information for other information and benefits everyday. Much has been written elsewhere about what citizens can do for themselves to restrict the circulation of personal

information about them. The Work Group concurs with the major theme that runs through this material — that individuals consider the privacy implications of engaging in day-to-day transactions in the marketplace.

There is no single solution to the vexing privacy challenges inherent in a digital, networked environment. Personal responsibility and proper government stewardship must be matched by meaningful privacy protections by the private sector if personally identifiable information is to be safeguarded when public records are released for commercial purposes.

It is difficult to overstate the importance of safeguards in the private sector. Given the massive volumes of information it accumulates, compounded by ever increasing capabilities to co-mingle once-discrete databases, the private sector is probably more important in terms of its impact on privacy than the governments from which it acquires information.

Government's increasing reliance on public-private partnerships and privatization has raised concerns in some circles about data integrity and personal privacy. In fact, as discussed below, legislative and contractual procedures are in place, although they vary from agency to agency — and program to program.

There is a strong case to be made for the competitive advantages of privacy protections in the private sector. Privacy advocates see this model as one way to help ensure the legal and authorized use of public records. Government could impose the same threshold for handling confidential records in the private sector as exists in the public sector — an oath of secrecy or contractual obligations to comply with privacy code in order to have continued access to the records. Representatives from the Polk Company and Commercial Information Systems (CIS) have told the Work Group that they have voluntarily imposed these kinds of restrictions on themselves.

Those who advocate the idea that there are competitive advantages derived through privacy protections in the private sector recognize that:

> [S]ome business needs legitimately require the collection of personal information. But the two goals of needing information for legitimate business purposes and privacy protection need not be mutually exclusive. Instead of competing against each other, the two can join forces if privacy-protective practices are built into one's business. In these times of fiercely competitive markets, if protecting consumer privacy is viewed as a component of good business practice, then privacy need not be treated as an adversary — it can be made an ally. When a company designs its products and services with privacy in mind, it also enhances the security of its information holdings, which in turn enhances customer confidence. That trust has considerable value.[91]

While this approach may seem counter-intuitive initially, it may be the basis of a self-correcting process over time. Dr. Cavoukian cautions that any self-correcting process will require external intervention to act as a catalyst to begin the necessary behavioral change. She said the private sector must be given a "nudge" to move in the right direction. Those "nudges" must come from a combination of public pressure and governmental direction.

Work Group members said the prospect of eventual self-correction should not prevent government from taking timely action to mitigate against possible harm to personal privacy.

VII. Research Disclosure

The Work Group recognizes there are frameworks in place to deal with sensitive records in specific areas. The procedures used for research

[91] Ibid: 185.

disclosure of confidential, electronic records may be instructive in developing a wider public policy framework.

State agencies receive frequent requests for disclosure of confidential records for research purposes. In some state agencies, requests made for research access are submitted to an institutional review board for consideration. Using a framework grounded in federal human subjects protection regulations,[92] the board reviews each request in terms of the scientific merit of the proposed research and the amount of "risk" involved in disclosing the confidential records. The board's decisions are binding, and may vary from denial of the request (e.g., the proposed study has no scientific merit) to disclosure with no conditions (e.g., the study is sound and needs only unidentifiable records), with many gradations in between.

Requests that involve a relatively high-risk disclosure of sensitive information are reviewed at a convened meeting of the board; the board may require the signed consent of the person to whom the record pertains as a condition for disclosure. Requests that are low-risk may be reviewed through an expedited process; in this case, the records could be disclosed without signed consent. Requests that do not involve disclosure of "identifiable" information may be reviewed and approved administratively by review board staff.

The institutional review board process for reviewing research requests for confidential records is a model available to all state agencies. Washington State agencies that are included in RCW 42.48 (Release of Records for Research) may disclose confidential electronic (or paper) records requested for research purposes under procedures defined in this law. These records are exempt from public disclosure under RCW 42.17.310, and thus their disclosure is at the agency's discretion. Further, under 42.48.030, the agency is allowed to impose reasonable charges to recover the costs of providing the records.

Under RCW 42.48.010, "state agency" currently means the Department of Social and Health Services, the Department of Corrections, institutions of higher education, and the Department of Health. The Health Care Authority has requested legislation to be added to this list.

Under RCW 42.48, a state agency may disclose confidential personal records for research purposes without the informed consent of the person to whom the records pertain if the agency has adopted human-research review and approval rules that include the appointment of a standing human research review board (i.e., institutional review board), and the review board determines:

- the disclosure request has scientific merit and is relevant to the agency's program concerns;
- the research would not be feasible without disclosure of the records in identifiable form and without waiver of informed consent;
- the disclosure risks have been minimized, and remaining risks are outweighed by anticipated health, safety, or scientific benefits;
- the disclosure does not violate federal law or regulation; and
- a legally binding confidentiality agreement is established between the researcher and the agency.

The researcher requesting access to the confidential electronic records must submit a research proposal for review and approval by the institutional review board. If the proposal is approved, review board staff draft the required confidentiality agreement. The agreement limits the disclosure to only those records that are needed for the research; extract files rather than source files are

[92] 45 CFR 46.

disclosed. The agreement also defines the limits on the use of the confidential records (they can only be used for purposes documented in the research proposal), defines the specific safeguards to ensure security and confidentiality, prohibits redisclosure of the records or record information, and requires the researcher to provide written certification to the agency that all identifiers have been destroyed when the research is completed. The agreement becomes effective when signed by the researcher and by the agency administrator responsible for the records to be disclosed.

The institutional review board requires that all changes in study plans be reviewed and approved in advance, and requires submission of annual progress reports for continued approval of the research.

Violation of the terms of the confidentiality agreement by either the researcher or the state agency is subject to a civil penalty of not more than $10,000 for each violation. In addition, unauthorized disclosure by the researcher who received the confidential records is a gross misdemeanor.[93]

VIII. Disclosure of Proprietary Business Information

As the Work Group examined issues related to the consistent handling of personally identifiable information in areas related to commercial access, a number of parties raised concerns about the uneven handling of proprietary business information.

Fully one third of the exemptions of the Open Records Act address the commercial sector. Yet, like some personally identifiable information, certain proprietary business information that is exempt from disclosure under one set of statutes is subject to disclosure under other statutes.

At issue is business information that derives independent economic value, actual or potential, from not being known to competitors or other persons who can obtain economic value from its disclosure and use. Any new measures to address this problem should not apply to the disclosure of statistical information aggregated from the proprietary business information in such a way that the submitting party or the details of the information are not identified.

In the Work Group's view, businesses should not be placed at a competitive disadvantage due to inconsistent disclosure provisions associated with state regulation and reporting requirements.

IX. Spanning the Gap: Government Action

Public comment before the Work Group reflected, in part, the hope that government can be trusted to protect personally identifiable information. In this respect, government must act as a barometer for public sentiment and concern.

Government Responsibility

Government often holds the unique authoritative record on matters of public concern — and intense personal consequence. The Work Group believes government must show leadership in safeguarding personal privacy. The rapid increases in unauthorized access to personally identifiable information via the Internet has prompted some to question the utility of limiting the circulation of such information from only one of many sources. However, when that single source is government, there are compelling reasons to provide safeguards:

- Public Trust: The Work Group believes that digital stewardship is foundational to the preservation of public trust and confidence in government. The Work Group also recognizes that

[93] RCW 42.48.050.

open government is a necessary pre-condition for public trust.

- Public Benefit: The Work Group has already explained its rationale for believing that the greatest public benefit is realized when public records are used within their "original orbit." Any public records released for commercial purposes should be limited to targeted use within their original orbit — that is, the purpose for which they were collected. General or secondary use of records should be restricted.

- Data Integrity: Privacy protections are likely to encourage individuals to provide more complete, current and — by extension — accurate information.

Government Action

Legislation

The Work Group favors legislative changes that would allow the "salting" of lists of individuals in order to identify abuse under the Open Records Act. Under current law, there are no penalties for agencies that improperly provide the list. There are no penalties if a company misrepresents how it will use the list or if it passes it on to a second party that uses the information to contact people on the list.

A white paper developed for the Work Group explained that businesses would be warned up front of possible penalties and the fact they could be sued for damages. The threat of loss of access to records would likely prove to be the greatest disincentive to commercial interests. In addition, the white paper suggested the introduction of financial disincentives for abuse, such as assessing a penalty on a per-name basis for each violation. As envisioned, the state would charge a penalty on a per-name basis for each violation. The potential for creating a financial disincentive is considerable given the size of the databases involved. Some databases contain thousands of names — other databases hold names that number in the millions.

The Work Group has also discussed the relative merits of revisiting the definitions in statute. There has been discussion about differentiating between public and private information in government records. There has also been discussion of creating a legal distinction between commercial and business use.

Finally, the Work Group's deliberations are coincident with at least three other activities in state government that touch on privacy issues:

- The Department of Licensing is requesting legislation to reconcile state law with provisions of the federal Driver's Identity Protection Act.

- There is a legislative proposal related to background checks provided through the Washington State Patrol.

- The Department of Licensing and the Washington State Patrol were directed by the Governor to "conduct a study regarding the feasibility and privacy implications of providing driver's license data to private entities."[94] The Governor has also asked that the study be delayed so the Work Group's findings could be taken into consideration.

Contractual Limitations

Agencies and authorized commercial interests enter into contractual agreements that define permissible use and prescribe penalties for abuse. The sanctions are often cast in terms of loss of access to the data. As a matter of practice, some commercial interests "salt" (or use tracers on) lists in their possession to ensure their customers are

[94] ESHB 2343 (Full Veto).

using the information in ways consistent with their contracts.

The larger information and marketing industries have responded to recent revelations about privacy breaches with increased reliance on independent audits and the introduction of voluntary privacy codes.

The Work Group believes there may be merit in providing for both "salting" of lists of individuals and compliance audits in structuring contracts between public entities and private sector information vendors.

System Design

Concurrent with the revolutionary development of electronic information technologies has come increasing public demand for electronic access to information generated and held by governments at all levels. By and large, government agencies have met this increasing demand with a full spectrum of reactions, ranging from deep concern and resistance to delight and frustration.

Availability, cost, and privacy are probably three of the four major issues to be addressed as governments move inexorably toward more electronic access to government information by the public (the fourth being commercial access). Of the four issues, privacy is probably of most concern to the public at large. Of course, if the disclosed information does not contain personally identifiable information, almost all privacy concerns disappear. Using current systems, providing access while protecting privacy to the extent provided in law is a problem for governments at all levels. However, information systems are modified, even replaced, at a faster rate than most government tools and other properties. As more and more government information is made available electonically, government agencies at all levels should give serious consideration to dealing wth the privacy issues by elevating privacy to a design element in new and modified systems.

With sufficient solidarity among government jurisdictions at the federal, state, and local levels, the vendor community would receive the message that this was to be a design element necessary in any system the government would purchase from them.

The difficulties and prohibitive costs associated with retrofitting existing computer systems with the capability to mask (or redact) personally identifiable information point to the need to build flexibility into system design at the ground floor. Governments and their private partners in commercial release should build privacy into all programs and systems at the design stage. An assessment of the cost of privacy provisions should be part of the decision package for new systems.

Washington State is by no means alone in its efforts to find privacy-friendly solutions in its handling of personally identifiable information. As a significant purchaser of information technology, government may be in a position to influence design decisions by vendors —making it clear that it will only buy those systems that safeguard privacy through the redaction of personally identifiable information or some other means.

X. Summary

In answering the question, *How can citizens be assured that personal information about them will be safeguarded when public records in electronic format are released for business or commercial purposes?*, the Work Group finds:

- privacy policies must seek to balance business and government needs for access to information with the individual's expectations of privacy.

- government has no interest in restricting access to information about the performance of public institutions or about public policy.
- government has a duty to safeguard the personally identifiable information of ordinary citizens from abuse. The duty extends to the notification of individuals of the procedures in place for the inspection of information held about them, pursuant to RCW 43.105.310.
- revelations about high-tech privacy breaches are fueling concern among citizens about the handling of their personally identifiable information.
- strong privacy protection can be a competitive advantage in the private sector.
- the public expects government to safeguard their personally identifiable information from inappropriate use.
- private-sector industry groups have responded to public concern by introducing voluntary codes of practice to protect privacy.
- the provision in Washington's Open Records Act to prohibit access to information "that is highly offensive to a reasonable person and of no legitimate public concern" is a very high threshold to meet in protecting privacy, but provides for relatively open access to records by the public.
- consistent with the code of *Fair Information Practices*, the collection of personal information should be limited to that which is necessary to fulfill legislative mandates of respective agencies.
- any public records released for commercial purposes should be limited to targeted use within their original orbit — that is, the purpose for which they were collected.
- general or secondary use of records should be restricted.
- after years of focusing on the automation process, there is a growing public concern about the combined effects of technological advances on personal privacy.
- government, the private sector and individuals all have roles to play in safeguarding personally identifiable information.
- strong privacy protection can be a competitive advantage in the private sector.
- the Work Group recommends legislative provisions to allow and possibly require the "salting" of lists to detect unauthorized use of lists of individuals, reinforced through an audit provision.
- contractual obligations with information resellers can increase accountability for unauthorized use.
- loss of access may be a more effective disincentive than monetary penalties alone.
- flexibility in the handling of personally identifiable information to meet a variety of access circumstances should be a basic and ubiquitous requirement for new systems design and for major system upgrades.

Public Stewardship

Chapter 5

Redirecting Taxpayer Subsidy to Commercial Access to Encourage, Support and Ensure Public Access

The Work Group's Answer to Question 3 in its Charter

If public records in electronic format are to be released for business or commercial purposes, how should the state allocate and recover costs?

I. Introduction

The allocation and recovery of costs related to commercial access represent important and controversial public policy issues, perhaps second only to those raised by questions of personal privacy. To be clear, the Work Group affirms that taxpayers should not pay to inspect information collected by government at taxpayer expense. Nor should charges for commercial access be used as a financial disincentive to limit the accountability of public institutions.

The Work Group also believes any cost recovery for commercial access must be based on allocating costs related to providing enhanced access — not the 'selling' of public records. In the Work Group's view, cost recovery for commercial access is not ultimately about generating new revenues — it is about being deliberate about what should be subsidized by tax dollars.

The allocation of costs associated with building and maintaining public electronic delivery systems for government information is an overriding concern of both government agencies and consumers. Government decision-makers are rightly concerned that the costs associated with building and maintaining public electronic delivery systems do not overly burden already-scarce government resources. Government and citizens are rightly concerned that electronic access to government information not impose greater costs to the end user, potentially widening the gap between the so-called "information haves" and "have-nots" based on their ability to pay.[95]

In recent years, Washington State policy makers have grappled with these funding issues. In 1994, the Legislature created the Public Information Access Policy Task Force,[96] to address public electronic access issues and recommend strategies for widespread electronic public access to government information. In its final report, the Task Force urged the Legislature to "clarify and resolve remaining costs, funding, and fees issues."[97]

For its part, the current Work Group was asked to address the narrow issue of cost recovery only as it relates to commercial access to government electronic records. The Work Group is concerned that policies which mandate that electronic government information be provided at low or no cost to commercial interests would in effect provide a substantial and largely invisible taxpayer subsidy of those commercial enterprises — even where most taxpayers will not use the electronic services and thus receive no offsetting public benefit.

The Work Group believes state information policies must balance the goals of broad electronic public access to government information with the government's need for such services to be economically viable, recognizing that electronic delivery systems will not develop fully without adequate provisions for cost recovery. Of course, where the Legislature makes a specific finding that a particular electronic service serves a broad public constituency and a compelling public interest, it can surely choose to fund services through legislative appropriations and not through user fees. However, where such funds have not been allocated, it is wholly appropriate for the state to consider cost-recovery options for commercial release.

[95] See, e.g., "A New Divide Between Have and Have-Nots?" Time Magazine On-Line at the URL: http://www.pathfinder.com/@@zRNJdwAAAAAAADgA/time/magazine/domestic/1995/special/special.society.html; "Principles on Public Information/Request for Comments," 60 Fed. Reg. 30609 (National Commission on Libraries and Information Science 1995).

[96] 1994 Wash. Laws Ch. 40, codified at RCW 42.17.261 (1994).

[97] Public Information Access Policy Task Force, *Report and Recommendations: Encouraging Widespread Public Electronic Access to Public Records and Information Held by State and Local Governments*, December 1, 1995: 16.

II. Public Stewardship in a Changing Environment

Data collected by the government and maintained in electronic format is the great undeveloped public resource of the 21st Century. It was created through public investment in technological infrastructure and it belongs to the people. The people have a fundamental right to the data for personal use and to monitor their government. To state it plainly, government must not interfere with individual access to data or access by the public for public purposes.

However, government must also realize that data is the means of production in an information society. Failure to recognize the economic value of data and to develop policies to ensure equitable exploitation will result in huge profits for a few at the expense of many.

It seems reasonable that government recover the cost associated with keeping data and the infrastructure that supports it current and useful. Without a coordinated and thoughtful policy on commercial access to government electronic records, government will continue to give away valuable public resources. Without public debate and a well-considered policy, 21st-Century taxpayers will continue to lose their public assets with the quiet efficiency only computer systems can produce.

The stakes in the new economy are enormous. By one estimate, sales of digital information in the United States generated $9.2 billion in 1990.[98] This industry, which has grown exponentially this decade with the advances in networked technology, does not need a taxpayer subsidy. Yet that is the effect of commercial release as it is now structured in many instances. As early adopters of new technologies, commercial interests benefit disproportionately from electronic information systems developed by government on behalf of the public. The subsidy is both large and largely invisible. It is reasonable to expect that taxpayers would receive some return on their investment when the IT systems built on their behalf are used for private gain.

At the same time, public-policy makers must resist the temptation to reverse the trend by establishing rates that are punitive to private-sector commercial interests. As has been established in the discussion of the first question, "legitimate business use" of public records provides some degree of public benefit. It is counterproductive to drive commercial providers out of a legitimate business use that furthers a public mission — directly or indirectly.

The key in this discussion is balance — a balance that results in what one witness called a "win-win-win" for government, business and the public. If the rate card skews high, business loses its motivation for being involved in such enterprises. If the rate card skews low, subsidies to commercial interests draw resources away from other government functions. A balanced rate card — where taxpayer subsidies to the commercial sector are unwound — provides equal commercial access to all competitors, furthers a public mission and eases demands on tax revenues.

III. Models for Cost Recovery

"Cost recovery" has been used in its generic sense by the Work Group and in the Governor's veto messages. It serves as a succinct shorthand for efforts to do what the terms suggests — recover the costs associated with providing information. In principle, an agency would recover all its costs and not draw resources away from its legislatively-mandated mission. In practice, full cost recovery is illusive. As documented in the agency survey conducted by the Work Group, agencies are able

[98] Ian Rowlands, "The Public-Private Debate Revisited," *Library and Information Research News*, Vol. 15, No. 54. (Summer, 1992), p. 24.

to offset costs to one degree or another but none are able to realize full cost recovery.

Some have contended that statutory provisions[99] prevent agencies from realizing full cost recovery, although there is an allowance for agencies to levy additional charges if they can be justified. That this allowance for justifying additional charges has gone virtually unused may point to a larger problem with which the information sector is still grappling.

Simply put, we do not know enough about information as an economic unit. The problem, according to Peter F. Drucker, is:

> [H]ow knowledge behaves as an economic resource, we do not yet fully understand; we have not had enough experience to formulate a theory to test it... We can, of course, estimate how much it costs to produce and distribute knowledge. But how much is produced ... we cannot say.[100]

Given the ambiguity concerning information as an economic resource, it may be helpful to be more precise in those areas where there is greater historic understanding. The shorthand of cost recovery does not allow a detailed understanding of the many approaches to assessing the value of information in an open economy.

With the assistance of experts from the industry and the academy, the Work Group engaged in wide-ranging discussion of funding options. The discussion that follows shifts the focus from cost recovery as a shorthand for an all-encompassing public policy objective to cost recovery as one of a number of approaches to be considered in attempting to reach that broader objective.

No Cost

Some agencies choose not to charge for information. The proliferation of agency home pages on the World Wide Web testifies to a concerted effort to communicate with the public at no cost in the electronic environment. A no-charge strategy can be effective in advancing an agency's policy objectives — particularly as they relate to public access and public information efforts.

However, the no-cost alternative for commercial access represents the highest possible level of taxpayer subsidy of business interests.

Cost Recovery

Cost recovery, narrowly defined here as a model for setting a fee schedule, bases pricing on the cost of production. The calculation includes the costs of making copies and handling charges. It may also include system-development costs and data-conversion costs. In some jurisdictions, system-maintenance costs are included in the calculation.

In Washington State, cost recovery for public access is confined largely to the cost of copying and related staff time.

The Work Group's survey of current practices documented widespread concern among agencies about cost recovery as it relates to commercial access. Agencies are concerned that cost recovery does not account for the need to stay abreast of technological advances over time. Cost recovery that is tied exclusively to the cost of production even for commercial access effectively precludes system refurbishment and improvements — the very improvements needed to meet the increasingly sophisticated demands of commercial users.

Agencies also reported difficulties in adapting a cost-recovery approach rooted in assumptions from paper-based records management to the new electronic environment. Fully 41 percent of respondents reported difficulty in tracking actual costs — including staff and computer-processing time — for all phases of processing a request.

[99] RCW 42.17.260 states:

(7) Each agency shall establish, maintain, and make available for public inspection and copying a statement of the actual per page cost or other costs, if any, that it charges for providing photocopies of public records and a statement of the factors and manner used to determine the actual per page cost or other costs, if any.

(a) In determining the actual per page cost for providing photocopies of public records, an agency may include all costs directly incident to copying such public records including the actual cost of the paper and the per page cost for use of agency copying equipment. In determining other actual costs for providing photocopies of public records, an agency may include all costs directly incident to shipping such public records, including the cost of postage or delivery charges and the cost of any container or envelope used.

(b) In determining the actual per page cost or other costs for providing copies of public records, an agency may not include staff salaries, benefits, or other general administrative or overhead charges, unless those costs are directly related to the actual cost of copying the public records. Staff time to copy and mail the requested public records may be included in an agency's costs.

(8) An agency need not calculate the actual per page cost or other costs it charges for providing photocopies of public records if to do so would be unduly burdensome, but in that event: The agency may not charge in excess of fifteen cents per page for photocopies of public records or for the use of agency equipment to photocopy public records and the actual postage or delivery charge and the cost of any container or envelope used to mail the public records to the requestor.

[100] Peter F. Drucker, *Post-Capitalist Society*, New York: Harper Business: 1993: 183, 185.

Value Pricing

Value pricing recognizes that users — particularly business users in the case of commercial access — all have different information needs and different resources. Under value pricing, rates are set based on the "value connected with the subjective evaluations of the individual information-seeker assessing how adequately the information content consulted meets his expectations and to what extent it is capable of satisfying his information needs."[101]

The subjective assessments by business users extend beyond supply and demand, and are based on convenience, the availability of alternatives and the benefits of the value-added information compared to other costs of doing business.

Value pricing has become a popular approach with the rise of digital technologies. Digital information often has more value to commercial users than the paper-based equivalent because of its malleability. Information in digital form can be easily customized to meet specific needs — and made available on demand, seven days a week, 24 hours a day.

The premiums associated with value pricing are often attractive to business users when compared to the costs of available alternatives. Despite initial resistance in some cases, testimony before the Work Group indicated that business users come to favor value pricing for the added convenience and, ultimately, cost savings. On-line, on-demand retrieval of records necessary for conducting business — even when value priced — cost a fraction of the cost of couriers and lost time associated with manual retrieval. In other words, the marginal costs to business of enhanced electronic access to government records often reduces the cost of doing business for private-sector enterprises. For example, the adoption of value pricing reduced the cost of receiving certain court records for a large-volume business user (Dunn and Bradstreet) from $1 per judgment to 40 cents.

In the Work Group's view, value pricing of information would be appropriate only in the context of commercial access. If the Legislature was to consider this model, it should include provisions whereby the revenues from value pricing for commercial access would be reapplied to support public access and refurbishing infrastructure.

Public-Private Partnerships

In testimony before the Work Group, commercial interests expressed the concern that public entities may have an unfair competitive advantage because of their legislative monopoly over data collection.

A number of state and local governments have found innovative ways to address this concern. As a recent article in Records Management Quarterly notes, "One policy option that seems to give publicly-funded agencies the advantages of selling information without the possibility of raising questions about unfair competitive practices is to have publicly-funded organizations sell their information by-products to consumers through a private sector agent."[102]

A model pioneered in Kansas[103] has been adopted by Indiana,[104] Arkansas,[105] and Nebraska.[106] An existing initiative in Georgia[107] is being refashioned around this model. Similar approaches are employed in New Mexico and by local governments in California.

The key characteristics of this model include:

- PUBLIC-PRIVATE PARTNERSHIP: The model relies on a public-private partnership that uses private capital, private employees and private initiative to expand government services. The model uses public regulation to safeguard the

[101] Reijo Savolainen, "Fee or Free?: The Socio-economic dimensions of the charging dilemma," *Journal of Information Science* 16 (1990): 146.

[102] Victoria Lemieux, "Selling information: what records managers should know," *Records Management Quarterly*, Vol. 30, No. 1; Pg. 3.

[103] Information Network of Kansas.

[104] Access Indiana Information Network.

[105] Information Network of Arkansas.

[106] Nebrask@ Online.

[107] GeorgiaNet.

public's interest from unfair monopoly or exploitation.

- CENTRALIZED BUT NON-EXCLUSIVE: The private partner has a non-exclusive license for state agency access. For their part, state agencies are able to refer inquiries to a central clearinghouse, thereby removing a significant workload from public servants. The central clearinghouse is a shared statewide resource that prevents duplicative and wasteful efforts by individual agencies to set up separate information-access systems.

- ENHANCED AND EQUAL COMMERCIAL ACCESS: The entities created by this model do not sell information, they sell enhanced access to public information. Commercial for-profit information resellers become customers — not competitors — of the partnership. Under such a plan, all of the commercial resellers enjoy equal access to the clearinghouse.

- CONVENIENCE: Commercial subscribers are willing to pay for the convenience and immediacy of accurate state public information — on an on-demand, as-needed basis.

- AGENCY OVERSIGHT/ PUBLIC OWNERSHIP: Public entities remain responsible for their data. The partnership agreement does not change the ownership of public records.

- PUBLIC ACCOUNTABILITY: Under partnership agreements, the state retains oversight of the clearinghouse but relinquishes day-to-day operation to the private partner. The partnership is constituted with a balanced board that represents public agencies, the private partner and users. The board works to anticipate and resolve problems.

- ENHANCED PUBLIC ACCESS: Public access to public information by electronic means is enhanced by the use of a properly managed public network. The network (or clearinghouse) provides public access to information for free — which really means it is subsidized by commercial access. For example, Access Indiana provides free access to 10,000 pages of information based on revenues from 15 pages for which there is a surcharge.

In testimony, Dr. Mark Haselkorn, Chair of the Department of Technical Communication within the College of Engineering at the University of Washington, told the Work Group that public-private partnerships focus attention on the question of "value" — where it resides, how it is added, by whom and under what circumstances. Partnerships effectively recast public infrastructure as a development environment for commercial interests that seek to repurpose public information. According to Haselkorn, in every case where products and services that rely on taxpayer-supplied infrastructure are brought to market, the relationship should be structured as a public-private partnership.

In related testimony before the Work Group, John Doktor of the Public Sector Marketing Group said a successful partnership requires both parties to recognize what each brings to the relationship. The public entity must guard against seeing the partnership solely in terms of an opportunity to shift risk to the private partner. For its part, the private partner must acknowledge the value that government brings to the relationship. The public entity is steward of unique, authoritative records — not simply a "raw resource" — and has an intimate knowledge of the collected data and the systems that support it.

Doktor, a self-described proponent of value pricing for commercial access, also told the Work Group that partnerships do not necessarily mean that risks and rewards are shared equally. Typically, greater risk is assumed by one partner. In such cases, the risk-bearing partner is allocated 80

percent of the benefit. Importantly, the other partner still receives 20 percent of the benefit, with any financial returns tied to the success of the partnership.

Washington State is clearly not alone in its efforts to adopt policies within its public mission that also reflect the fundamental shifts that come with the emerging information-based economy.

The Work Group also believes that there are two conventional economic models that are not consistent with proper public stewardship of public records — optimal and marginal cost pricing.

- Optimal Pricing assigns value to information based on what the market will bear — with no consideration given to the cost of producing the product or non-monetary benefits of moderating the cost. The propriety of such a market-driven approach in the context of an agency's public mission is suspect. Further, a strategy to maximize profits (while wholly appropriate in the private sector) does not fit well with the primary public-sector motivation for commercial access — generating revenue to maintain or improve service levels.

- Marginal-Cost Pricing also focuses on what the market will bear, calculating that the marginal cost of producing an additional unit of a product is equal to the amount of additional revenue that is to be gained by selling an additional unit. Unlike optimal pricing, marginal-cost pricing does account for the cost of production but does not lend itself to the public-purpose dynamic at the core of public records management.

The Work Group encourages the Legislature to incorporate structures that protect and promote the value of public infrastructure to the commercial information sector.

Until such time that information is better understood as an economic unit, public entities can mitigate risk by taking at least four steps:

1. Contracts with the private-sector for information should be non-exclusive in nature. Exclusive contractual arrangement may thwart innovation and competition in the private sector.

2. Contracts should have a limited-time horizon. Long-term contracts limit government's ability to adapt to change and correct oversights in the original arrangement.

3. Contracts should contain certain safeguards on personally identifiable information, with sanctions clearly articulated.

4. Contracts should not confer ownership of public records on any third party. Public records are held as a public trust and government, as steward, must retain ownership rights and responsibilities for the data.

IV. Distinguishing Records from Delivery

The creation of documents should be distinguished from their delivery. The government is the public trustee of all records it creates or maintains. Under the Open Records Act, a person has the right to examine all public records except those that fall into categories specifically exempted from disclosure.[108] The creation of those documents is publicly financed insofar as citizens have paid for the public office, personnel, pencils, paper, and computers to make them. Having paid for them once, it is appropriate that the public be entitled, as it is under the Open Records Act, to inspect the records at no cost.[109]

By contrast, reproduction and delivery of government data and information present their own

[108] As amended in 1992, the Act states:

> The people of this state do not yield their sovereignty to the agencies that serve them. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created. The public records subdivision of this chapter shall be liberally construed and its exemptions narrowly construed to promote this public policy.

RCW 42.17.251 (1994). The Act exempts from disclosure 33 categories of government documents, including personal information in files of public school students, hospital patients, welfare recipients, public agency employees and appointed or elected officials. See, for example, RCW 42.17.310 (1994).

[109] RCW 42.17.300 (1994).

cost considerations. With regard to reproduction, Washington State law specifically authorizes agencies to impose "a reasonable charge for providing copies of public records and the use by any person of agency equipment to copy public records, which charges shall not exceed the amount necessary to reimburse the agency for actual costs of the copying."[110] With regard to delivery, current state law requires agencies to "honor requests received by mail,"[111] but does not require them to absorb the costs of photocopying or delivering the information to the requester. Although most agencies absorb postage costs for all but the most voluminous requests, they generally do not pay the delivery costs where a requester elects, for example, to use courier service, overnight mail, or fax to ensure faster delivery. Electronic access is, like a courier service, a speedier and more convenient form of delivery.

It appears from the context of the Open Records Act that "actual costs" as used therein does refer to incremental costs of processing requests for public records. A 1991 Washington Attorney General's opinion stated that actual costs as used in the Act "could include such items as the costs of the copying machine (including maintenance); paper and other supplies; and staff time devoted to the copying process. The agency must be able to justify its charges based on these and other direct costs."[112] The same opinion found that records search fees were not allowable, since they were not "incidental to copying," but pertained to inspection of public records. "[I]t would be incongruous to impose search fees as 'incidental' to copying, when inspection of those same records must be free."[113] This opinion, then, makes a clear distinction between inspection of public records, which is free, and obtaining copies, which is not.

Moreover, while the Open Records Act makes clear that electronic records are public records,[114] it does not mandate that government provide for inspection in the most convenient manner regardless of costs. Washington State law requires only that "[r]esponses to requests for public records shall be made promptly by agencies."[115] The Attorney General has stated that in determining whether an agency has responded "promptly" to a document request — including the steps of "deleting or redacting the portions of each record that the agency determines should be withheld from disclosure" — "courts will take into account the agency's resources, the nature of the request and the content of the records requested."[116] Where an agency's resources do not allow for electronic public delivery systems, or where they do not provide for firewalls on systems initially designed for internal agency use, the less-costly process of manually redacting records is legally sufficient, even though it may be far less prompt and less convenient to the requester. From this perspective, electronic redaction goes to the convenience of delivery, not to the search and inspection of public records. Once again, a policy which bars an agency from recouping funding for the necessary security components of an information system undermines the agencies' ability to develop these more convenient information systems in the first place.

Of course, where an agency uses an information service for both internal use and public electronic access, it should separate the costs of each. For example, if an agency has a photocopier for internal use but uses this machine to copy a document in responding to an open records request, the incremental costs would only reflect the actual cost of the paper, ink and toner used for the photocopy, and that percentage of the cost and maintenance of the photocopier directly apportionable to satisfying the documents request, and not attributable to the agency as overhead for its internal operations. However, if a government's internal operations do not require a public access component, the additional costs of developing the system to accommodate public access must also

[110] Id.

[111] RCW 42.17.270 (1994).

[112] Public Records — Initiative No. 276, 1991 Op. Att'y Gen. 6, at 6 (emphasis added). Amendments to RCW 42.17.260(8) in 1995 imposed a 15 cent per page limit.

[113] Id. at 5-6.

[114] RCW 42.17.020(27) defines "Public record" as including "any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." RCW 42.17.020(29), in turn, defines "writing" to mean "every... means of recording any form of communication or representation, including, but not limited to, words, pictures, sounds or symbols, or combinations thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film, and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated."

[115] RCW 42.17.320 (1994).

[116] 1991 Op. Att'y Gen. 6, at 4.

be included within incremental costs. James Love of the Washington, D.C.-based Taxpayer Assets Project notes that where governments' internal needs would be met without public access services, incremental costs of providing public access would be explained in the equation ICP = C (P,G) - C (G), where C (P,G) is the cost of both the internal use (G) and public access (P), and C(G) is the cost of internal use only.[117] Under this equation, the costs of public interfaces, firewalls, and other components which must be added to provide public electronic access, all come within incremental costs.

Delivery can take many forms, from first-class mail delivery of paper or electronic documents (e.g., on disk or cartridge) to electronic delivery over the most costly computer-networking systems. While there are potential public benefits that may stem from electronic delivery of government records, it does not follow that all electronic delivery systems need be made available to all citizens in all cases to further either the general public interest or a specific government objective. Where particular delivery systems would primarily serve a narrow constituency, and not the public as a whole, a fee-recovery mechanism may be appropriate. Even where a system may have a broader public demand, user fees may be appropriate so long as they do not work to create improper barriers to public access.

V. Redirecting Public Subsidies for Commercial Access

There is no such thing as "free" electronic access. The design, development, deployment, and refurbishment of public electronic delivery systems require significant investments[118] which must come from some source, whether it is a private grant, legislative appropriation, existing agency budget or user fee. Determining the appropriate kinds of electronic delivery to provide requires an assessment of the specific government objective, the extent and nature of consumer demand, and the best and most cost-efficient technology for the job.

Demand for Government Information

Beyond specific categories where widespread public demand is readily acknowledged, there is often little widespread public demand for particular kinds of information; what additional demand that exists comes from narrow and specific constituencies, usually commercial entities seeking information for resale or attorneys seeking information for litigation purposes.

In 1994, a survey by the Office of Financial Management reported that 59 percent of state agencies surveyed reported requests for data for commercial purposes, while 47 percent have received requests for litigation purposes.[119] In 1996, the Work Group survey found that 85 percent of state agencies surveyed reported requests for data for commercial purposes, while 68 percent have received requests for litigation purposes.

Cost recovery, then, should focus on these regular commercial users. For example, large commercial users (who are often resellers of government information) directly invest substantial funds to acquire, format, analyze, and distribute government information over broad geographic areas to a diverse customer base. In addition, specialty commercial resellers of public records invest in highly targeted categories of records to format, analyze, and provide information to a highly select customer base. These users require specialized analysis that is generally of a commercial nature and has a high financial value; they add value through their understanding of the specific business needs of the select customer base to which they provide service. In each case the costs of electronic delivery of the raw government data has a

---

[117] James Love, "Pricing Government Information," *Journal of Govt. Information* 22, no. 5 (1995): 363-387. The ACLU of Washington calls for a careful accounting of incremental costs, but would allow the imposition of user fees to cover them. "[I]f fees must be charged, the total revenue must be no greater than sufficient to cover the incremental costs of providing electronic or other new forms of access." ACLU of Washington, *Policy on On-Line Access to Government Information*, July 17, 1993 (hereafter "ACLU Policy") at 2.

[118] For example, the costs of making portions of an internal legislative database available to the public exceeded $75,000, and requires another $58,000 annually to cover operating costs. Washington State Legislative Service Center, *A Briefing on the Legislature's Public Access Systems*, January 1995.

[119] Helberg Memo, *supra* at n. 18.

high commercial value to a specific audience but very little to the larger public.

Agencies should not be precluded from developing sustainable fee-based services for the commercial sector where a broad public interest that would justify public funding has not been established. In these cases, direct fees to users are the fairer form of recovering costs, since only those who use a service are burdened with paying for it. By contrast, direct public funding of electronic delivery systems may be inappropriate, since in many cases it would be a taxpayer subsidy to commercial entities who use government information for profit.

Availability of Legislative Funding

Public subsidies require allocations of scarce resources. They are used most widely to support the legislatively mandated missions of state agencies. The Legislature must be increasingly deliberate in choosing where to target its allocations. Given spending restrictions placed on state government, subsidies to commercial access may come at the expense of other government services.

First, to provide appropriations for electronic access without reducing funds for other government programs assumes an increase in total government funding. Where there is no growth in state funding, appropriations for electronic delivery of government information must be made at the expense of existing programs. Indeed, Washington State is subject to the limits of Initiative 601, passed by voters in 1994, which limits the amount of money the Legislature can spend without turning to the voters for approval. In its first 18 months, it bans any tax increase without a public vote. After that, it establishes a spending cap for state government — based on a formula which factors in population growth and inflation — and requires a supermajority of the Legislature (60 percent) and voter approval to exceed the cap.[120] In this environment, agencies which seek legislative appropriations to provide such new services in effect ask the government to take attention and resources away from existing projects. Even were Washington State not subject to Initiative 601, it must be recognized that electronic access is not a service that has traditionally been provided by government. Therefore it is unlikely that the Legislature would significantly decrease funding for existing programs to make room for the now-higher priority electronic access projects. In this environment, electronic access services will simply not be developed or implemented.

Second, where development and deployment of services is wholly dependent upon legislative appropriations, there is no certainty that funding, even if approved one year, will be sustained in the next. Several examples are illustrative. In Hawaii, the Legislature in 1995 terminated the Hawaii Interactive Network Corporation, or "Hawaii INC," a publicly-owned gateway and videotex service, citing high costs.[121] In California, the Legislature defunded the Info/California electronic kiosk project, citing high costs and dissatisfaction with content.[122] Contrast these struggling initiatives with the burgeoning public-private partnerships discussed above in Kansas, Indiana, Arkansas and Nebraska that serve multiple constituencies through a system whereby commercial access cross-subsidizes public access.

VI. Ensuring That Fees Do Not Inhibit Public Access

The objectives of public electronic access, as set forth by the Legislature,[123] are not incompatible with direct assessment of fees on users. The goals of government efficiency, strategic management of government resources, and citizen access may be best assured by a policy that recognizes the need for agency flexibility in developing sus-

[120] B. Ellis, "Washington Splits in Tax Initiatives," *The* (Portland) *Oregonian,* November 3, 1993: A1.

[121] V. Viotti, "Budget cuts force Hawaii INC to close," *Honolulu Advertiser,* July 26, 1995: 1.

[122] D. Bernstein, "Agencies That Escape Cuts Despite Loud, Long Criticism," *Sacramento Bee,* April 24, 1995: A11.

[123] The Legislature found that government information is a strategic resource and needs to be managed as such and that broad public access to non-restricted public information and records must be guaranteed. The legislature further finds that reengineering government processes along with capitalizing in advancements made in digital technology can build greater efficiencies in government service delivery. The legislature further finds that providing citizen electronic access to presently available public documents will allow increased citizen involvement in state policies and empower citizens to participate in state policy decision making.

tainable funding mechanisms, but assures that such mechanisms do not create undue barriers to the public's ability to use electronic delivery service, either by charging fees that make the services unaffordable to most users or by requiring that they have expensive equipment to access them. Rather than limit user fees outright, state policy should set forth criteria to provide guidance to agencies considering user fees to ensure that the public's interest in such services is protected.

Specifically, agency determinations of fees for electronic access services should address three basic points: First, the establishment of fee-based electronic services must be viewed as an addition to, and not a substitute for, free non-electronic access to government records now provided under the Open Records Act. Second, where fees are assessed, fee structures should be determined with a limited goal of achieving sustainable funding for the service itself (including regular upgrading and refurbishment of public infrastructure); not of providing an additional revenue source for unrelated agency activities. Such a cap seeks to ensure that fee structures do not unduly preclude access to significant numbers of users, especially non-profit organizations and individuals. Third, any electronic-access delivery mechanism should provide some level of free electronic access through terminals or kiosks located in public facilities such as schools or libraries. A policy encompassing these points would allow governments to develop potentially sustainable sources of funding for services which allow them to recover agency costs and, at the same time, further public goals of electronic access by subsidizing and improving low-cost or no-cost access services.

There are several ways to structure user fees to mitigate further the concern that electronic delivery of government information will be unavailable to citizens who need it. For example, agencies may establish graduated-fee schedules based on the volume of use, so as to allow less-expensive access to occasional or low-volume users. They may also vary fees according to the time of day a service is accessed, such as setting lower fees after conventional working hours or on weekends.

The most common way is to establish differential pricing which imposes higher fees on high-volume commercial customers than on others. The American Civil Liberties Union (ACLU) of Washington recommended to the Public Access Information Policy Task Force that fees for commercial users cross-subsidize public access by individuals, non-profit organizations, and schools. "Fees charged to large volume commercial users may be greater than the cost of providing access to those users, as long as the surplus is used to subsidize access to those exempted from fees."[124] Jane Nelson, administrator for the Washington courts and a former Task Force member, has also noted that "wide-scale and inexpensive public access ... may require outlays of funds for equipment which could be financed by charging commercial enterprises higher prices for 'wholesale' access."[125] Indeed, such user fees for commercial entities could go far to implement the earlier Task Force's call for the public to have "at least one avenue of no cost access to the highest caliber version of any publicly funded government information system that serves an outside constituency, perhaps through access to the state's officially designated depository libraries."[126]

Reasonable and standardized user fees dedicated to improving public electronic information services would not impose undue economic burdens on commercial concerns. For one thing, these companies generally pass the fees on to their commercial customers. For another, they would still have the option of obtaining documents or electronic records through mail or in person, or, depending on the fee structure, through evening or weekend access when user fees might be lower. In

[124] ACLU Policy, at 2.

[125] Jane W. Nelson, "The Public's Records: Public Records Policy in the Information Age," presented to the American Association of Law Librarians, July 31, 1995.

[126] PIAPTF Final Report, p 8.

any event, where user fees are limited to the development, maintenance, and refurbishment costs of public electronic services, it can also be expected that in many cases fees would decline over time as the government recovers its development costs.

VII. Summary

In answering the question, *If public records in electronic format are to be released for business or commercial purposes, how should the state allocate and recover costs?*, the Work Group finds:

- the public should not pay to inspect information collected by government at taxpayer expense.
- financial disincentives should not be used to restrict access to government.
- cost recovery is based on providing enhanced access, not the 'selling' of public records.
- requiring agencies to provide electronic delivery of information at below-incremental cost potentially retards the development of new systems since there is no ready funding source for the development, enhancement and eventual refurbishment of the networked infrastructure that makes commercial access possible.
- government must be deliberate in developing a model for cost recovery that provides for sharing risks and sharing rewards.
- government is not a passive holder of information, but a development environment which adds value to the information that is ultimately of commercial interest.
- providing low- or no-cost access to commercial enterprises would effectively provide a substantial and largely invisible taxpayer subsidy of those enterprises — even where most taxpayers will not use the electronic services and thus receive no offsetting public benefit.
- public-private partnerships, where the value added by both partners is recognized, may be an effective means to recoup taxpayer cost which would otherwise be provided as subsidies to commercial enterprises.
- beyond issues related to personally identifiable information, proprietary business information provided to government as a condition of license or reporting requirement is treated unevenly from agency to agency. Such information may be exempt from disclosure under statute at one agency but open to disclosure at another, leaving the business at a potential competitive disadvantage.

Acknowledgments

Lead Staff

Paul W. Taylor
Department of Information Services
Work Group Staff Coordinator

Fred Hellberg
Office of Financial Management
Chair, Work Group Staff
Support Group

Carol Poole
Office of Financial Management

The Work Group gratefully acknowledges the assistance of the following individuals:

Bretta Beveridge
Steve Bleecker
Jim Booker
Linda Bremer
Tim Brown
Eric Campbell
Jim Culp
David Danner
Cindy Davis
Lenore Doyle
Becky Egan
Sheri Evans
Marilyn Freeman
Michael Flint
Sarah Garmire
Julia Graham
Mike Gotta
Dave Hastings
Jami Heinricher-Brock
Larry Hewitt
Emily Hill
Jeff Holm
Teresa Jennings
George Kotch
Kerri Kroll
David McDonald
Janet McLane
Teresa Morris
Martin Munguia
Rhonda Penrose
Sheila Perry
Rhonda Polidori
George Scott
Todd Sander
Mary Lou Smith
Curt Stucki
John Swannack
Elizabeth Ward

Appendices

Commercial Access To Government Electronic Records

Testimony Before the Work Group

Appendix A

At its public hearings, the Work Group heard from a wide cross-section of interested parties, including the newspaper industry, commercial information resellers, private-sector interests that rely on information to do business, technology consultants, privacy advocates, community activists, and representatives of state and local governments:

- Michael Killeen, Attorney, Davis Wright Tremaine
- Glenn Jacobs, Commercial Information Systems, Inc.
- Glenn Anderson, Commercial Information Systems, Inc.
- Theodore (Ted) Hotham, R. L. Polk Company
- John Doktor, The Public Sector Marketing Group, Inc.
- Larry Berg, Lawyer, CyberArtists
- Ann Cavoukian, Assistant Privacy Commissioner, Province of Ontario, and co-author of *Who Knows: Safeguarding Your Privacy in a Networked World*
- Jerry Sheehan, Legislative Director, American Civil Liberties Union of Washington (ACLU-W)
- Dr. Karen J. Sy, University of Washington, member of the *Public Information Access Policy Task Force.*
- Mark Haselkorn, College of Engineering, University of Washington
- Emily Hill, Public Records Officer, University of Washington
- Jim Justin, Association of Washington Cities
- Debbie Wilke, County Officials Association
- Linda Moran, Assistant Attorney General, Departments of Licensing and Employment Security
- John Swannack, Deputy Director, Department of Licensing
- Tim Brown, Chief, Research and Data Analysis, Department of Social and Health Services
- Elizabeth Ward, Assistant Director, Epidemiology and Health Statistics, Department of Health
- Todd Sander, Department of Information Services

Appendix B

Written Submissions to the Work Group

In addition to public comment from private citizens, the Work Group received written submissions from a number of business interests — ranging from financial institutions and law firms to retailers and service companies:

- James T. Serres, Commercial Information Systems, Inc.
- Theodore D. Hotham, R.L. Polk & Company
- Ron Sailer, Automated Business Services, Inc.
- Tremaine Smith, Department of Revenue (in response to Mr. Sailer's concerns)
- Joellen R. Thompson, Credit Union of the Pacific
- David P. Marosi, Marosi & Associates, Inc.
- Thomas L. Ray, Northwest Protective Service, Inc.
- Gary Gross, Northwest Protective Service, Inc.
- Dan Reeves, Superior Tire Service
- John Henry Hingson III, Attorney at Law
- Harold D. Gillis, Gleaves, Swearingen, Larson, Potter & Smith
- Rodney B. Wheeland, National Association of Credit Management
- John A. Velk, Fred Meyer, Inc.
- David R. Ambrose, Ambrose & Associates, P.C.
- Jo Ann Langford, Rams Specialized Security Service
- Mark W. Hope, Waste Recovery, Inc.
- Al Krueger, The Estey Corporation
- Kerry P. Zeiler, Western States Association for Investigator's Advocacy
- Linda L. Hoyer, Hoyer & Associates
- Douglas H. Cole, The Bartell Drug Company
- Elaine Guard, Barrett Business Services, Inc.
- Tom Koecke, Pierce County Chapter Counseling & Collections, Inc.
- Steve Boles, Les Schwab Tire Centers
- Michael J. Canaan, Trident Investigative Services, Inc.
- Robert T. Mac Onie, Jr., Washington State Section, American Congress on Surveying & Mapping
- Rowland Thompson, Allied Daily Newspapers of Washington
- Tom Koenninger, *The Columbian*
- Beth Givens, Privacy Rights Clearinghouse, University of San Diego.

Compilation of State Statutes

Appendix C

A compilation of state statutes concerning the exemption of software as a public record, privacy and cost recovery.

State	Software Exemption	Privacy	Cost Recovery
Alaska	Software developed by an agency or a contractor is subject to the statutory fee schedule. sec. 09.25.220.	44.99.300 Fair information Practices law creates a process for citizen to challenge the accuracy of personal information subject to public disclosure. Agencies must notify data subject of: 1. law permitting information 2. consequences of not providing information 3. anticipated use and disclosure of the data 4. how to challenge the accuracy	Not to exceed the standard unit cost of duplication; if production of records for one requester in a calendar month exceeds five person-hours, the public agency shall require the requester to pay the personnel costs required during the month to complete the search and copying tasks. ss 09.25.115 for electronic services and products may charge actual incremental costs and a reasonable portion of costs of development & maintenance of public agency system. ss 09.25.115(f) When offering on-line access for fee, agency must also provide public terminal at no charge.
California	Software developed by a state or local agency is not a public record. The agency may sell, lease, or license the software for commercial or non-commercial use. sec. 6254.9.	Civil Code Sec. 1798 Fair Information Practices Act gives citizens right to see and correct state files about themselves. State agencies may disclose personal information only in limited circumstances. Law permits invasion-of-privacy lawsuits against a person who intentionally discloses personal information that was known to come from a state or federal agency in violation of law. Motor vehicle registration information may be sold at cost, but buyer must identify the reason for the request. Data is freely available to press and an attorney, but there is a 10 day wait for person requesting access to another person's motor vehicle records.	Government ss 6256 Must provide copies of "identifiable record" ss 6257 Covering direct costs of duplication or a statutory fee, if applicable. ss 408.3 & ss 409 for "property characteristics information," assessor may charge fee related to the actual cost of developing and providing the information. Development costs may include overhead, personnel, supplies, material, office, storage, and computer costs. ss 408.3 & ss 409 Only applies to counties with population over 715,000 ss 6256 Public agency has choice in which form computer data will be provided.

Colorado	Software is specifically not included in definition of public writing. sec. 24-72-202(7). Agencies may obtain and enforce trademark or copyright protection for any public record, except that public access shall not be restricted. sec. 24-72-203.	24-27-204 Individuals are permitted to examine their own records, but state must keep following records confidential: medical and personnel files, library material; address and telephone number of public school students.	ss 24-72-205(1) Reasonable fee not to exceed $1.25/page unless actual cost exceeds that. ss 24-72-205(4) If computer output other than word processing, the fee may be based on recovery of actual incremental costs of providing the electronic services and products together with a reasonable portion of the costs associated with building and maintaining the information system. Judicial decisions have cleared the way for user fees.
Connecticut		4-190 State and local Government are to maintain only necessary information and provide individual access to such information. Agencies must keep a record of disclosures.	Not to exceed $1.00 for the first page and $.50/additional page. ss 1-19a, eff. July 1, 1992, permits special fees for computer-stored records. Such fees may include hourly salary, and charges for computer time. ss 1-19a eff. July 1, 1992, no public agency may enter into any contract if such contract impairs the right of public access to records stored on a computer system.
Florida	Data processing software is included in the definition of public record. sec. 119.011. Any agency may copyright its data processing software. The agency may make revenue from the software unless it is used solely for understanding the agency's data. ch. 119.083. Software obtained under a licensing agreement and which is a trade secret and "sensitive software" developed by an agency are also exempt. ch. 119.07(1)(q).	282.318 State departments must have information security manager to assure that security procedures for data processing are followed.	As prescribed by law; if not prescribed $.15 per one-sided copy up to 14"X8 1/2"; actual cost for other sides. ss 119.085 allows a fee to be charged for electronic access which includes the direct and indirect costs of providing user access. ss 119.07(b) a special service charge may be added for requests which require extensive use of information technology resources.
Georgia	The statute exempts computer programs or software used or maintained in the course of operation of a public office or agency. sec. 50-18-72(f)(2).		$.25/page unless otherwise provided by law; In addition, a reasonable charge may be collected for search, retrieval, and other direct administrative costs provided no charge is made for the first quarter hour. Op. Atty Gen. 89-32 Information does not fall outside Open Records Act because it is stored by magnetic tape or diskette Georgia Planning Act of 1989 establishes funds for database development; joint funding with USEPA

Hawaii	The legislature owns all rights, titles, and interests in all legislatively-generated databases, including software. sec. 21D-4.	92F Uniform Information Practices Act permits individuals to have access to "personal records" about themselves. Privacy interests must be balanced against public interest in disclosure of medical, social service, financial and performance evaluation data. Individuals may correct errors. Office of Information Practices within the Department of the Attorney General enforces the law.	ss 92F-42(13) Fees may be set by the director of information practices for searching, reviewing, or segregating discloseable record. ss 92F-11(c) Unless the information is readily retrievable by the agency in the form in which it requested, an agency shall not be required to prepare a compilation or summary of its records.
Idaho	Computer programs developed or purchased by an agency are generally exempt. sec. 9-340(16). Computer programs which are trade secrets are exempt entirely. sec. 9-340(2).	ss 9-338(8) Unless another fee is provided by law, a fee not to exceed the actual cost to the agency of copying. Actual costs do not include any administrative or labor cost. For a duplicate of a computer tape, a fee may be charged not to exceed the sum of the agency's direct cost and the standard cost, if any, for selling the same information in the form of a publication. ss 9-340(16) Exemption from disclosure for computer programs does not include a compilation or through manipulation of the original data produced by use of the program. ss 39-120 Supports GIS use for Water Resources.	
Illinois	"Administrative or technical information associated with automated data processing operation" may be withheld, including software. data. 140/7(p).	116.43.5 Most state records are public, others may be disclosed if the requester signs an affidavit "that the information shall not be made available to other persons." Public records law includes language: "Nothing in this section shall require the Secretary of State to invade or assist in the invasion of any person's right to privacy."	ss 206 Actual costs for copying and for the use of equipment to copy records, excluding costs of search and review, unless otherwise provided by statue. ss 201 State FOIA is not intended to be used for the furthering of a commercial enterprise or to disrupt the work of a public body. Nor is the Act intended to create an obligation to prepare any public record which was not prepared when the Act became effective. Federal Surface Mining and Reclamation Act; III Rev. Statute III supports GIS for solid waste planning.

Indiana	An agency may withhold computer programs, code, and other software that are owned by the agency or entrusted to it. sec. 5-14-3-4(b)(11).	4-1-6 Fair Information Practices Act requires that state agencies may determine when personal information may be exchanged Citizen has a right to inspect personal information except medical records; however, agencies define whether personal data is confidential or public.	ss 5-14-3-8 Not to exceed $.10/ page for standard size documents of reasonable fee for non-standard-size. For a duplicate of a computer tape a fee may be charged, not to exceed the sum of the agency's direct cost and the standard cost, if any, for selling the same information in the form of a publication. ss 36-1-3-8(6) Applicable to local government units where user fees are permitted but which restricts such fees to what is reasonable and just. ss I.C.2-5-19 Creates Census Data Advisory Committee.
Kansas	Software programs for electronic data processing are exempt. sec. 45-221.		ss 45-219(c) Not to exceed actual cost, including cost of staff time and computer services ss 45-221(35) Can refuse request if it places an unreasonable burden on agency ss 45-220(c)(2) Cannot use lists of names and addresses for sales or sell the list.
Kentucky	Software is included in the definition of public record, however software is defined not to include "specific addresses of files, passwords, access codes, user identifications, or any other mechanism for controlling the security or restricting access to public records." sec. 61-870(3)(a).	61.870 State open records law mandates access to any and all records of public agencies except records of personal nature, certain law enforcement records and a few other categories. Provision is made that persons shall have access to public records relating to them.	ss 61.874(3) A public agency may impose a reasonable fee for the creation of non-standardized services and products available through a database or GIS. ss 61.970 Person who requests a copy of all or any part of a database or a geographic information system, in any form for a commercial purpose must provide certified statement on commercial purpose of use of data and enter into a contract with owner of the database or GIS for a specified fee based on: a) Cost to the agency of time, equipment and personnel in production of database or GIS. b) Cost to agency for creation or acquisition of database or GIS. c) Value of commercial purpose for which database or GIS is to be used. ss 61.975 the fee for copies of records stored on a database or a GIS and not requested for a commercial purpose shall not exceed the actual costs of copying. ss 7.510 State may charge for electronic access to legislative electronic information system.

Louisiana	Software is exempt when it is part of "any automated broker interface system or any automated manifest systems." sec. 44:4(13).		ss 44-32 Reasonable Title 50, ss 71 Provides for a statewide land information mapping and records system.
Maine		5.1851 Bureau of Central Computer Services established to effect consolidation of data processing equipment and to safeguard confidentiality of information files.	The cost of complying Also; whenever inspection of public data cannot be accomplished without translation of electronic data into some other form the person desiring inspection may be required to pay the cost of translation ss 1753-A5. Office of Geographic Information Systems may levy appropriate charges for use of GIS services ss 1756 GIS data are subject to licensing agreements and are only available upon payment of fees pursuant to this chapter.
Massachusetts		66A Agency must designate individual responsible for personal data systems and must enact regulation governing outside access and individual challenge and correction Each personal data system must be registered with the secretary of state.	Reasonable fee including the actual expense of a search.
Michigan	Computer software is not a public record and may be withheld. 79 Mich. Op. Att'y Gen. 5500 (1979).		ss 15.123 Fees limited to the actual mailing costs, and actual cost of duplication including labor, the cost of search, examination, review and the deletion and separation of exempt from non-exempt from non-exempt material[sic] ss 15.122(3)&(4) The Act does not require a public body to make a compilation, summary, or report, nor to create a new public record.

Minnesota	An agency may copyright computer software, therefore making it exempt as a trade secret. sec. 13.03. The Minnesota Government Information Access council has issued recommendations that would restrict the use of copyright by state and local government units, but would allow some government works, including software, to be copyrighted. Minn. Gov't Info. Access Council, *Report on Minnesota Government Use of Copyright and Intellectual Property (1996).*	13.01 Data Practices Act covers state agencies and institutions, school boards, local commissions but not townships. Defines confidential personal data not available to the individual. Each agency must designate a person to be responsible for data banks and report annually to state department of administration. Individual must be told purpose and use of information and has a right to contest personal information before action taken against them due to "Computer matching"	Reasonable and actual costs of copying, searching and retrieving. For requests which involve the receipt of information that has commercial value and is a substantial and discreet portion of a formula, pattern, compilation, program, device, method, technique, process, data base or system developed with a significant expenditure of public funds, a reasonable fee related to the actual development costs may be charged. ss 375.85 A county may market self-developed computer programs. Such programs are considered trade secrets of the governmental entity.
Mississippi	Computer software programs developed by the state are not subject to the act. Miss. Op. Att'y Gen. (April 3, 1992). Data processing software which is either a trade secret or is "sensitive" is not subject to inspection, copying, or reproduction. sec 25-61-9 (6).	25-53-55 If "confidential information" is wrongfully released to a state agency, the person may complain to the central data processing authority and charges may be brought against employee involved.	ss 25-61-7 Reasonably calculated to reimburse the public body but in no case to exceed the actual cost of searching, reviewing and/or duplicating.
Missouri	Records are exempt if they relate to "software codes for electronic data processing and documentation thereof." sec. 610-021(10).		Reasonable rate ss 610.026 Not exceeding the actual cost of document search and duplication. Fees for providing access to records on computer facilities may include only the cost of copies and staff time required for making copies. ss 115.157 An election authority may sell printouts of voter lists.
Nevada	State owned or licensed software is not a public record. 89 Nev. Op. Att'y Gen. 1 (1989).		ss 239.030 Such fees as may be prescribed for the services of copying.
New Hampshire		7-A Information Practices Act requires data banks Maintained by state agencies to be registered with the state department of administration.	91-A:IV Actual cost of providing copy.

New Mexico	No statutory provision regarding software. However, NM Technet, the private organization which provides on-line access to public records, often copyrights software it has developed for an agency and then licenses it back to the agency. Any software which is not copyrighted becomes public domain. Fla. Jt. Comm. on Info. Tech'y Resources, *Agency Created Data Processing Software as a Public Record 66 (1993).*		ss 14-2-2 Custodian of records must provide facilities for making memoranda abstracts from records. No direct provision for copies except for veterans. No general provision for fees. ss 15-1-9 Upon payment of a reasonable fee, information contained in an information systems database can be disclosed in printed form. A fee may be charged for access or use of the database for any private or non-public use. ss 15-1-9C In order to obtain a copy of a data base in computer or printed form a person must agree to not make unauthorized copies of the data base and not to use the data base for any political or commercial purpose unless the use is approved by the state agency.
New York	No statutory provision regarding software.	91 "each agency maintaining a system of records shall prepare a notice describing each of its systems of records," including the uses made of each category of records and the disclosures of personal information that the agency regularly makes. The Committee on Public Access to Records is responsible for registering all state agency data banks, to take citizen complaints, and to issue advisory opinions. Citizens have a right to see and correct their own files.	Upon written request for a record reasonably described 87(b) $.25 for standard sized records, not to exceed actual cost for other records.
North Carolina	"Nothing in this section requires a public agency to disclose its software security, including passwords." sec. 132-6.1(c).		ss 102-17 County projects shall be eligible for assistance subject to availability of funds, compliance with administrative regulations and conformity with one or more of the project outlines.
North Dakota	The statute excludes trade secrets including "computer software program[s] and components of... computer software program[s]." sec. 44-04-18.4. In addition, any computer program or software for which an agency obtains a copyright is confidential. sec. 44-04-18.5.		

Ohio		1346.01 Notice stating the nature and character of any personal information system and name of individual directly responsible for it must be filed with the director of administrative services. Agencies maintaining theses systems must inform persons whether the information they are asked to provide is legally required and must collect only personal information necessary and relevant to the functions of that agency. With certain specific exemptions, personal information may not be disclosed without the consent of the individual. The law provides for accessing, challenging and amending one's own record	ss 149.43 Every public office must (1) allow any person to inspect all public records at reasonable times during regular business hours; (2) make copies of public records available, at cost, and within a reasonable amount of time; and (3) organize its records so that they may be accessed within a reasonable period of time.
Oklahoma	The statute excludes trade secrets including "computer software program[s] and components of...computer software program[s]." sec. 44-04-18.4. In addition, any computer program or software for which an agency obtains a copyright is confidential. sec. 44-04-18.5.	74.118.17 Data Processing Planning and Management Act provides for storage of confidential data in centralized data processing center to preclude access without authorization	ss 24A5.3 $.25/page for standard sized documents. If the request is solely for a commercial purpose then a reasonable fee may be charged. ss 24A.10B.3 If disclosure would give an unfair advantage to competitors, a public body may keep confidential computer programs or software "but not the data."
Oregon	"Computer programs developed for or purchased by or for any public body for its own use" are exempt. sec 192.501(16). See previous column.		Fees reasonably calculated to reimburse the actual cost in making the record available. ss 192.501(16) Specifically provides that analyses, compilations and other manipulated forms of data produced by the use of a computer program are not exempt from disclosure. ss 192.502 Intergovernmental group's geographic databases or systems are confidential and exempt from public disclosure. ss 190.050 Intergovernmental groups are prohibited from restricting access to public records through the inclusion of such records in a geographic database or system.

Texas	A statute exempts from public records requirements "the data base," defined as, "the machine readable form of the material prepared for and used in the publication of the administrative code." sec. 2002.056 The Attorney General determined that the source code and documentation for software is not covered by the act. 90 Texas Op. Att'y Gen. ORD-581 (1990).		
Utah	Computer programs and software are exempt from the Act if developed by the agency for its own use. sec 63-2-103(18)(b)(viii). Agencies may own an intellectual property right in any material. sec. 63-2-201(10)(a).	63-2-103 Government Records Access and Management Act includes principles of fair information practices found in federal privacy act. Types of data collected by state agencies are reported annually. There are four categories of personal information: public, private, confidential, and protected. Individuals have the right to contest the accuracy of their own data.	ss 63-2-203 May charge a reasonable fee covering the actual cost of duplication or compiling a record in a form other than that in which it is maintained. May not charge a fee for reviewing a record. ss 63-2-201(5) A governmental agency is not required to create a record in response to a request. A record shall be provided in a particular format if it can be done without unreasonably interfering with government duties and the requester pays any additional costs actually incurred. ss 63-2-201(7) A governmental entity which offers a copyrighted or patented record for sale may control the access, duplication, and distribution of the material. Automated Geographic Reference Center created.
Virginia	Computer software developed by or for a state agency or political subdivision may be exempted at the record custodian's discretion. sec. 2.1-342(B)(24).	2.1-377 Privacy Protection Act of 1976 prohibits secret personal information systems and collection of unneeded, inappropriate, inaccurate information. Law provides for access and correction.	ss 2.1-342.4 Reasonable charges for copying, search times and computer time, not to exceed the actual cost to the public body in supplying such records, except that a public body may charge on a pro rata per acre basis for the cost of creating topographical maps for such maps which encompass a contiguous area greater than 50 acres. Computer data must be made available at a reasonable cost. Public bodies are not required to create a record if it does not already exist. Virginia Geographic Information Network funded.

Washington		*Open Records Act* RCW 42.17.255 *Invasion of Privacy, when*. A person's "right to privacy," "right of privacy," "privacy," or "personal privacy," as these terms are used in this chapter, is invaded or violated only if disclosure of information about the person: (1) Would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public. The provisions of this chapter dealing with the right to privacy in certain public records do not create any right of privacy beyond those rights that are specified in this chapter as express exemptions from the public's right to inspect, examine, or copy public records. [1987 c 403 d 2.] Intent — 1987 c 403: "The legislature intends to restore the law relating to the release of public records largely to that which existed prior to the Washington Supreme Court decision in "*In Re Rosier*," 105 Wn.2d 606 (1986). The intent of this legislation is to make clear that: (1) Absent statutory provisions to the contrary, agencies possessing records should in responding to requests for disclosure not make any distinctions in releasing or not releasing records based upon the identity of the person or agency which requested the records, and (2) agencies having public records should rely only upon statutory exemptions or prohibitions for refusal to provide public records. Further, to avoid unnecessary confusion, "privacy" as used in RCW 42.17.255 is intended to have the same meaning as the definition given that word by the Supreme Court in "Hearst v. Hoppe," 90 Wn2d 123,135 (1978)." [1987 c 403 d 1.] *Violating Right of Privacy.* RCW 9.73.030 Intercepting, recording or divulging private communication — Consent required — Exceptions.	*Open Records Act* RCW 42.17.260 (7) Each agency shall establish, maintain, and make available for public inspection and copying a statement of the actual per page cost or other costs, if any, that it charges for providing photocopies of public records and a statement of the factors and manner used to determine the actual per page cost or other costs, if any. (a) In determining the actual per page cost for providing photocopies of public records, an agency may include all costs directly incident to copying such public records including the actual cost of the paper and the per page cost for use of agency copying equipment. In determining other actual costs for providing photocopies of public records, an agency may include all costs directly incident to shopping such public records, including the cost of postage or delivery charges and the cost of any container or envelope used. (b) In determining the actual per page cost or other costs for providing copies of public records, an agency may not include staff salaries, benefits, or other general administrative or overhead charges, unless those costs are directly related to the actual cost of copying the public records. Staff time to copy and mail the requested public records may be included in an agency's costs. (8) An agency need not calculate the actual per page cost or other costs it charges for providing photocopies of public records if to do so would be unduly burdensome, but in that event: The agency may not charge in excess of fifteen cents per page for photocopies of public records or for the use of agency equipment to photocopy public records and the actual postage or delivery charge and the cost of any container or envelope used to mail the public records to the requestor.

		(1) Except as otherwise provided in this chapter, it shall be unlawful for any individual, partnership, corporation, association, or the state of Wash-ington, its agencies, and political subdivisions to intercept, or record any: (a) Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication; (b) Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all the persons engaged in the conversation. *Telecommunications* RCW 80.36.400 Automatic dialing and announcing device — Commercial Solicitation by. (1) As used in this section: (a) An automatic dialing and announcing device is a device which automatically dials telephone numbers and plays a recorded message once a connection is made. (b) Commercial solicitation means the unsolicited initiation of a telephone conversation for the purpose of encouraging a person to purchase property, goods, or services. (2) No person may use an automatic dialing and announcing device for purposes of commercial solicitation. This section applies to all commercial solicitation intended to be received by telephone customers within the state. (3) A violation of this section is a violation of chapter 19.86.RCW. It shall be presumed that damages to the recipient of commercial solicitations made using an automatic dialing and announcing device are five hundred dollars. (4) Nothing in this section shall be construed to prevent the	*Public Access* *41.105.280 Electronic access to public records — costs and fees.* Funding to meet the costs of providing access, including the building of the necessary information systems, the digitizing of information, developing the ability to mask nondisclosable information, and maintenance and upgrade of information access systems should come primarily from state and local appropriations, federal dollars, grants, private funds, cooperative ventures among governments, nonexclusive licensing, and public/private partnerships. Agencies should not offer customized electronic access services as the primary way of responding to requests or as a primary source of revenue. Fees for staff time to respond to requests, and other direct costs may be included in costs of providing customized access. Agencies and local governments are encouraged to pool resources and to form cooperative ventures to provide electronic access to government records and information. State agencies are encouraged to seek federal and private grants for projects that provide increased efficiency and improve government delivery of information and services. [1996 c 171 d 12.]

Washington utilities and transportation commission from adopting additional rules regulating automatic dialing and announcing devices. [1986 c 281 d 2.]
Legislative finding — 1986 c 281: "The legislature finds that the use of automatic dialing and announcing devices for purposes of commercial solicitation: (1) Deprives consumers of the opportunity to immediately question a seller about the veracity of their claims; (2) subjects consumers to unwarranted invasions of their privacy; and (3) encourages inefficient and potentially harmful use of the telephone network. The legislature further finds that it is in the public interest to prohibit the use of automatic dialing and announcing devices for purposes of commercial solicitation." [1986 c 281 d 1.]

RCW 80.36.540 Telefacsimile messages — Unsolicited transmission — Penalties
(1) As used in this section, "telefacsimile message" means the transmittal of electronic signals over telephone lines for conversion into written text. (2) No person, corporation, partnership, or association shall initiate the unsolicited transmission of telefacsimile messages promoting goods or services for purchase by the recipient. (3) (a) Except as provided in (b) of this subsection, this section shall not apply to telefacsimile messages sent to a recipient with whom the initiator has had a prior contractual or business relationship.
(b) A person shall not initiate an unsolicited telefacsimile message under the provisions of (a) of this subsection if the person knew or reasonably should have known that the recipient is a governmental entity. (4) Not–withstanding subsection (3) of this section, it is unlawful to initiate any telefacsimile message to a recipient who has previously sent a written or telefacsimile message to the

initiator clearly indicating that the recipient does not want to receive telefacsimile messages from the initiator. (5) The unsolicited transmission of telefacsimile messages promoting goods or services for purchase by the recipient is a matter affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86. RCW. The transmission of unsolicited telefacsimile messages is not reasonable in relation to the development and preservation of business. A violation of this section is an unfair or deceptive act in trade or commerce for the purpose of apply-ing the consumer protection act, chapter 19.86 RCW. Damages to the recipient of telefacsimile messages in violation of this section are $500 or actual damages, whichever is greater.

Unemployment Compensation — Records and Information - Privacy and Confidentiality RCW 50.13.010 Legislative intent and recognition. This chapter is intended to reconcile the free access to public records granted by the open government act and the discovery rights of judicial and administrative systems with the historical confidentiality of certain records of the department of employment security and the individual's right of privacy as acknowledged by the open government act.

The legislature recognized that records and information held by the department of employment security could be misused. Therefore, this chapter defines a right of privacy and confidentiality as regards individual and employing said records maintained by the department of employment security. The legislature further recognizes that there are situations where this right of privacy and confidentiality is outweighed by other consider-ations. Therefore, this chapter also defines certain exceptions to the right of privacy and confidentiality. [1977 ex.s. c 153 d 1.]

Wisconsin	Computer programs are exempt, but not "material produced as a product of the program." sec. 19.36(4).	Ch.19 Seven-person Privacy Council appoints a privacy advocate to present the privacy perspective instate policy making and to assist citizens in access to their own files. State agencies must register their records and develop rules of conduct for handling of personal data. Individual must be notified before adverse action is taken as result of computer matching unless the state or local agency finds the information used "sufficiently reliable." The 1995 Wisconsin Legislature eliminated the Privacy Council and abolished the Privacy Advocate position. In their place, a more narrowly-focused Telecommunications Privacy Council has been created to monitor citizen concerns and complaints on behalf of the state utilities and telecommunications commission. The remaining functions of the Council and Advocate have been transferred to the Department of Administration.	ss 19.35(1) The actual, necessary and direct cost of reproduction may be imposed, unless a fee is otherwise established by law. ss 19.35(g) Right to obtain copy does not apply to a record which has been or will be promptly published with copies offered for sale or distribution. ss 19.35(1) The act does not require an authority to create a new record by extracting information from existing records and compiling the information in a new format. 59.88 Land record Modernization Funding. Portion of recording fees used to support land modernization activities.

Compiled from:

Anneliese May. DRAFT: "Access to Electronic Public Information: A Summary of Current Trends." National Conference of State Legislatures (NCSL), July 1996.

Citizen Access to Local Government Infostructure: A Guide to Public Policy Makers, by Clay Wirt, A project of State League Directors, National League of Cities and Public Technology, Inc., 1995.

Compilation of State and Federal Privacy Laws, by Robert Ellis Smith with James S. Sulanowski, Published by Privacy Journal, 1992.

For What It's Worth: A Guide to Valuing and Pricing Local Government Information, Public Technology, Inc., 1996.

Statute Law Committee, *1996 Revised Code of Washington (RCW)*, 8 Volumes, Olympia, WA: 1996.

Survey of State Open Records and Privacy Laws, GIS Law, Volume 3, Number 1: 21-27.

HB 2790: Full Text & Veto Message

Appendix D

An Act relating to distribution of certain governmental lists and information

House Bill 2790 — Full Text
AS AMENDED BY THE SENATE
Passed Legislature - 1996 Regular Session
State of Washington 54th Legislature 1996 Regular Session

By Representatives Dyer, Hymes, Scott, Wolfe, Honeyford, D. Schmidt and B. Thomas

Read first time 01/19/96. Trade and Economic Development.

AN ACT Relating to distribution of certain governmental lists and information; amending RCW 46.12.370 and 82.32.330; adding new sections to chapter 42.17 RCW; and adding a new section to chapter 82.32 RCW.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

RCW 46.12.370 and 1982 c 215 s 1 are each amended to read as follows:

In addition to any other authority which it may have, the department of licensing may furnish lists of registered and legal owners of motor vehicles only for the purposes specified in this section to:

(1) The manufacturers of motor vehicles, or their authorized agents, to be used to enable those manufacturers to carry out the provisions of the National Traffic and Motor Vehicle Safety Act of 1966 (15 U.S.C. sec. 1382-1418), including amendments or additions thereto, respecting safety-related defects in motor vehicles;

(2) Any governmental agency of the United States or Canada, or political subdivisions thereof, to be used by it or by its authorized commercial agents or contractors only in connection with the enforcement of motor vehicle or traffic laws by, or programs related to traffic safety of, that government agency. Only such parts of the list as are required for completion of the work required of the agent or contractor shall be provided to such agent or contractor; ((or))

(3) Any business regularly making loans to other persons to finance the purchase of motor vehicles, to be used to assist the person requesting the list to determine ownership of specific vehicles for the purpose of determining whether or not to provide such financing. In the event a list of registered and legal owners of motor vehicles is used for any purpose other than that authorized in subsections (1)((, (2) and (3))) through (4) of this section, the manufacturer, governmental agency, financial institution or their authorized agents or contractors responsible for the unauthorized disclosure or use will be denied further access to such information by the department of licensing; or

(4) To private companies that provide on-line computer data base services to federal, state, and local agencies for law enforcement or government purposes. The department shall first obtain the written agreement and assurances satisfactory to the agency of any company requesting information under this section that any list so obtained shall not be provided to any person other than as provided in this section.

A new section is added to chapter 42.17 RCW to read as follows:

In addition to the provisions of RCW 42.17.260, state agencies may furnish lists that they maintain of public information, including such lists in computer readable form or on magnetic tape, that they make available to other federal, state, or local government agencies, including law enforcement agencies, to private companies that provide on-line computer data base services with data bases consisting primarily of public records. An agency shall first obtain the written agreement and assur-

ances of the data base company satisfactory to the agency that the company will supply the lists and information so obtained only to federal, state, or local government agencies solely for law enforcement or governmental purposes.

RCW 82.32.330 and 1995 c 197 s 1 are each amended to read as follows:

(1) For purposes of this section:

(a) "Disclose" means to make known to any person in any manner whatever a return or tax information;

(b) "Return" means a tax or information return or claim for refund required by, or provided for or permitted under, the laws of this state which is filed with the department of revenue by, on behalf of, or with respect to a person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists that are supplemental to, or part of, the return so filed;

(c) "Tax information" means (i) a taxpayer's identity, (ii) the nature, source, or amount of the axpayer's income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability deficiencies, overassessments, or tax payments, whether taken from he taxpayer's books and records or any other source, (iii) whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, (iv) a part of a written determination that is not designated as a precedent and disclosed pursuant to RCW 82.32.410, or a background file document relating to a written determination, and (v) other data received by, recorded by, prepared by, furnished to, or collected by the department of revenue with respect to the determination of the existence, or possible existence, of liability, or the amount thereof, of a person under the laws of this state for a tax, penalty, interest, fine, forfeiture, or other imposition, or offense: PROVIDED, That data, material, or documents that do not disclose information related to a specific or identifiable taxpayer do not constitute tax information under this section. Except as provided by RCW 82.32.410, nothing in this chapter shall require any person possessing data, material, or documents made confidential and privileged by this section to delete information from such data, material, or documents so as to permit its disclosure;

(d) "State agency" means every Washington state office, department, division, bureau, board, commission, or other state agency;

(e) "Taxpayer identity" means the taxpayer's name, address, telephone number, registration number, or any combination thereof, or any other information disclosing the identity of the taxpayer; and

(f) "Department" means the department of revenue or its officer, agent, employee, or representative.

(2) Returns and tax information shall be confidential and privileged, and except as authorized by this section, neither the department of revenue nor any other person may disclose any return or tax information.

(3) The foregoing, however, shall not prohibit the department of revenue from:

(a) Disclosing such return or tax information in a civil or criminal judicial proceeding or an administrative proceeding:

(i) In respect of any tax imposed under the laws of this state if the taxpayer or its officer or other person liable under Title 82 RCW is a party in the proceeding; or

(ii) In which the taxpayer about whom such return or tax information is sought and another state agency are adverse parties in the proceeding;

(b) Disclosing, subject to such requirements and conditions as the director shall prescribe by rules adopted pursuant to chapter 34.05 RCW, such return or tax information regarding a taxpayer to such taxpayer or to such person or persons as that taxpayer may designate in a request for, or consent to, such disclosure, or to any other person, at the taxpayer's request, to the extent necessary to comply with a request for information or assistance made by the taxpayer to such other person: PROVIDED, That tax information not received from taxpayer shall not be so disclosed if the director determines that such disclosure would compromise any investigation or litigation by any federal, state, or local government agency in connection with the civil or criminal liability of the taxpayer disclosure would identify a confidential informant, or that such disclosure is agreement entered into by the department that provides for the reciprocal exchange of information with other government agencies which agreement requires respect to such information unless such information is required to be disclosed to the taxpayer by the order of any court;

(c) Disclosing the name of a taxpayer with a deficiency greater than five thousand dollars and against whom a warrant under RCW 82.32.210 has been either issued or filed and remains outstanding for a period of at least ten working days. required to disclose any information under this subsection if a taxpayer: (i) Has been issued a tax assessment; (ii) has been issued a warrant that has not been filed; and (iii) has entered a deferred payment arrangement with the department of revenue and is making payments upon such deficiency that will fully satisfy the indebtedness within twelve months;

(d) Disclosing the name of a taxpayer with a deficiency greater than five thousand dollars and against whom a warrant under RCW 82.32.210 has been filed with a court of record and remains outstanding;

(e) Publishing statistics so classified as to prevent the identification of particular returns or reports or items thereof;

(f) Disclosing such return or tax information, for official purposes only, to the governor or attorney general, or to any state agency, or to any committee or legislature dealing with matters of taxation, revenue, trade, commerce, the control industry or the professions;

(g) Permitting the department of revenue's records to be audited and proper state officer, his or her agents and employees;

(h) Disclosing any such return or tax information to the proper officer of the internal revenue service of the United States, the Canadian government or provincial governments of Canada, or to the proper officer of the tax department of any state or city or town or county, for official purposes, but only if the statutes of the United States, Canada or its provincial governments, or of such other state be, grants substantially similar privileges to the proper officers of this state;

(i) Disclosing any such return or tax information to the Department of Alcohol, Tobacco and Firearms of the Department of the Treasury, the Department of Defense, the United States customs service, the coast guard of the United States, and the United States department of transportation, or any authorized representative thereof, for official purposes;

(j) Publishing or otherwise disclosing the text of a written determination designated by the director as a precedent pursuant to RCW 82.32.410;

(k) Disclosing, in a manner that is not associated with other tax information, the taxpayer name, entity type, business address, mailing address, rev-

enue tax registration numbers, standard industrial classification code of a taxpayer, and the dates of opening and closing of business. This subsection shall not be construed as giving authority to the department to give, sell, or provide access to any list of taxpayers for any commercial purpose except as provided in section 4 of this act; or

(l) Disclosing such return or tax information that is also maintained by another Washington state or local governmental agency as a public record available for inspection and copying under the provisions of chapter 42.17 RCW or is a document maintained by a court of record not otherwise prohibited from disclosure

(4) (a) The department may disclose return or taxpayer information to a person under investigation or during any court or administrative proceeding against a person under investigation as provided in this subsection (4). The disclosure must be in connection with, the department's official duties relating to an audit, collection activity, or a civil or criminal investigation. The disclosure may occur only when the person under investigation and the person in possession of data, materials, or documents are parties to the return or tax information to be disclosed. The department may disclose return or tax information such as invoices, contracts, bills, statements, resale or exemption certificates, or checks. However, the department may not disclose general ledgers, sales or cash receipt journals, check registers, accounts receivable/payable ledgers, general journals, financial statements, expert's workpapers, income tax returns, state tax returns, tax return workpapers, or other similar data, materials, or documents.

(b) Before disclosure of any tax return or tax information under this subsection (4), the department shall, through written correspondence, inform the person in possession of the data, materials, or documents to be disclosed. The correspondence shall clearly identify the data, materials, or documents to be disclosed. The department may not disclose any tax return or tax information under this subsection (4) until the time period allowed in (c) of this subsection has expired or until the court has ruled on any challenge brought under (c) of this subsection.

(c) The person in possession of the data, materials, or documents to be disclosed by the department has twenty days from the receipt of the written request required under (b) of this subsection to petition the superior court of the county in which the petitioner resides for injunctive relief. The court shall limit or deny the request of the department if the court determines that:

(i) The data, materials, or documents sought for disclosure are cumulative or duplicative, or are obtainable from some other source that is more convenient, less burdensome, or less expensive;

(ii) The production of the data, materials, or documents sought would be unduly burdensome or expensive, taking into account the needs of the department, the amount in controversy, limitations on the petitioner's resources, and the importance of the issues at stake; or

(iii) The data, materials, or documents sought for disclosure contain trade secret information that, if disclosed, could harm the petitioner.

(d) The department shall reimburse reasonable expenses for the production of data, materials, or documents incurred by the person in possession of the data, materials, or documents to be disclosed.

(e) Requesting information under (b) of this subsection that may indicate that a taxpayer is under investigation does not constitute a disclosure of tax return or tax information under this section.

(5) Any person acquiring knowledge of any return or tax information in the course of his or her employment with the department of revenue and any person acquiring knowledge of any return or tax information as provided under subsection (3)(f), (g), (h), or (i) of this section, who discloses any such return or tax information to another person not entitled to knowledge of such return or tax information under the provisions of this section, shall upon conviction be punished by a fine not exceeding one thousand dollars and, if the person guilty of such violation is an officer or employee of the state, such person shall forfeit such office or employment and shall be incapable of holding any public office or employment in this state for a period of two years thereafter.

A new section is added to chapter 82.32 RCW to read as follows:

The department of revenue may furnish lists of taxpayer names, entity types, business addresses, mailing addresses, revenue tax registration numbers, standard industrial classification code of taxpayer, and the dates of opening and closing of a business to companies that provide on-line computer data base services. The on-line computer companies shall provide the data bases consisting primarily of public records only to other federal, state, or local government agencies solely for law enforcement or government purposes. Before providing a list to a company under this section, the department shall obtain a written agreement that any list so provided shall be used only for the purposes specified in this section.

A new section is added to chapter 42.17 RCW to read as follows:

The legislature finds that the practices covered by RCW 46.12.370(4) and sections 2 and 4 of this act are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. Violations of RCW 46.12.370(4) and sections 2 and 4 of this act are not reasonable in relation to the development and preservation of business. A violation of RCW 46.12.370(4) or section 2 or 4 of this act is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

— END —

Veto Message on HB 2790
March 30, 1996
To the Honorable Speaker and Members,
The House of Representatives of the State
of Washington

Ladies and Gentlemen:

I am returning herewith, without my approval, House Bill No. 2790 entitled:

"AN ACT Relating to distribution of certain governmental lists and information;" House Bill No. 2790 expands the permitted use of public records for commercial purposes. In certain circumstances it allows the Departments of Licensing and Revenue, as well as other agencies, to release information to private companies that provide on-line computer services to government agencies. This information would include lists in computer readable form or on magnetic tape.

The underlying law regarding the commercial use of records was established by an act of the people when they passed Initiative 276 in 1972. That initiative provided for access to public records in ways that would allow citizens to hold their government more accountable, but the use of lists for commercial purposes was generally prohibited. The initiative provided that "[t]his law shall not be construed as giving authority to any agency to give, sell or provide access to lists of individuals requested for commercial purposes, and agencies shall not do so unless specifically authorized or

directed by law" (Initiative 276, Section 25 (5)). Specific legislative authorizations for

the commercial use of lists have proliferated since 1972, a process that House Bill No. 2790 would continue.

The issue here is not only one of privacy, but also of the value and purpose of governmental records. The government collects an immense amount of information from its citizens and from businesses. Much of the information is required for specific purposes, but we try to limit those purposes to the administration of programs, the development of policies, and the collection of revenues - all things that promote the common good. As the economy becomes increasingly service-oriented and as the impact of electronic information systems becomes more pervasive, there is great pressure placed on government to relinquish public control over its data holdings to the benefit of private, commercial enterprises.

In the instance of House Bill No. 2790, the state is being asked to provide its information at cost or for nothing. The company is then contemplating selling that information back to the state for a profit. This raises serious issues that state policy now fails to answer. Does the governmental data base have a commercial value that should be considered an asset of the state? If it is to be used for commercial reasons at all, should the state share in whatever profit comes from the use of its data?

Should the individual citizen who supplied the data or who is the subject of the file or list have a right to decide what commercial use should be made of his or her records?

House Bill No. 2790 may, by itself, promote a useful purpose. However, when viewed in combination with the myriad of requests for access to the public record that are being introduced into each legislative session, this bill raises serious questions about what our policy should be regarding the commercialization of the government's data holdings. Our state must develop a clear, comprehensive policy about this issue lest the passage of bills like this one continue to erode away, in a piecemeal fashion, the policy established by a vote of the people in 1972.

In order that a comprehensive policy governing the commercial use of public records can be developed, I will soon appoint a task force to address this issue. Consideration also will be given to issues associated with privacy. This task force will consist of persons who can help advise the executive and legislative branches about this important matter. I will ask the task force to prepare recommendations that can be debated in the 1997 and in subsequent legislative sessions.

By raising the issue this year through the exercise of this veto and others, I am aware that I will be asking our policy makers to undertake a task that will bring into focus a complicated debate that will reveal conflicting values about public records, privacy, the future of technology, and governmental accountability. However, I am determined that this important debate go forward and that important principles of government not be determined by a process wherein the slow accumulation of exceptions to the underlying law become so extensive that more data is available for commercial uses than is withheld.

For these reasons, I have vetoed House Bill No. 2790 in its entirety.

Respectfully submitted,
Mike Lowry
Governor

HB 2604: Full Text & Veto Message

Appendix E

An Act relating to lists of registered and legal owners of vehicles

House Bill 2604 — Full Text
Passed Legislature - 1996 Regular Session
State of Washington 54th Legislature 1996 Regular Session By Representatives Silver, R. Fisher, Chopp and Tokuda

Read first time 01/15/96. Referred to Committee on Transportation.

AN ACT Relating to lists of registered and legal owners of vehicles; and amending RCW 46.12.370.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

1. RCW 46.12.370 and 1982 c 215 s 1 are each amended to read as follows: In addition to any other authority which it may have, the department of licensing may furnish lists of registered and legal owners of motor vehicles only for the purposes specified in this section to:

(1) The manufacturers of motor vehicles, or their authorized agents, to be used to enable those manufacturers to carry out the provisions of the National Traffic and Motor Vehicle Safety Act of 1966 (15 U.S.C. sec. 1382-1418), including amendments or additions thereto, respecting safety-related defects in motor vehicles;

(2) Any governmental agency of the United States or Canada, or political subdivisions thereof, to be used by it or by its authorized commercial agents or contractors only in connection with the enforcement of motor vehicle or traffic laws by, or programs related to traffic safety of, that government agency. Only such parts of the list as are required for completion of the work required of the agent or contractor shall be provided to such agent or contractor; ((or))

(3) A commercial parking company requiring the names and addresses of registered owners to notify them of outstanding parking violations. The department may provide only the parts of the list that are required for completion of the work required of the company; or

(4) Any business regularly making loans to other persons to finance the purchase of motor vehicles, to be used to assist the person requesting the list to determine ownership of specific vehicles for the purpose of determining whether or not to provide such financing.

In the event a list of registered and legal owners of motor vehicles is used for any purpose other than that authorized in ((subsections (1), (2) and (3) of)) this section, the manufacturer, governmental agency, commercial parking company, financial institution, or their authorized agents or contractors responsible for the unauthorized disclosure or use will be denied further access to such information by the department of licensing.

— END —

Veto Message on HB 2604
March 30, 1996
To the Honorable Speaker and Members,
The House of Representatives of the
State of Washington
Ladies and Gentlemen:

I am returning herewith, without my approval, House Bill No. 2604 entitled:

"AN ACT Relating to lists of registered and legal owners of vehicles;"

House Bill No. 2604 provides the operators of commercial parking companies electronic access to the records of the Department of Licensing so that they may use those records to identify the owners of automobiles who used their parking lots without providing sufficient payment. Presently, these companies can access these records only through means which they argue are more expensive and cumbersome.

House Bill No. 2604 raises a much larger issue than would appear on the surface. Our state has not developed a clear policy about how and why public records should be accessed for commercial purposes. The underlying law regarding the commercial use of records was established by an act of the people when they passed Initiative 276 in 1972. That initiative provided for access to public records in ways that would allow citizens to hold their government more accountable, but the use of lists for commercial purposes was generally prohibited. The initiative provided that "[t]his law shall not be construed as giving authority to any agency to give, sell or provide access to lists of individuals requested for commercial purposes, and agencies shall not do so unless specifically authorized or directed by law" (Initiative 276, Section 25 (5)). Specific legislative authorizations for the commercial use of lists have proliferated since 1972, a process that House Bill No. 2604 would continue.

The issue here is not only one of privacy, but also of the value and purpose of governmental records. The government collects an immense amount of information from its citizens and from businesses. Much of the information is required for specific purposes related to the administration of programs, the development of policies, and the collection of revenues - all things that promote the common good. As the economy becomes increasingly service-oriented and as the impact of electronic information systems becomes more pervasive, great pressure is placed on the government to relinquish public control over its data holdings to the benefit of private, commercial enterprises.

As state government responds to emerging technologies, it is likely that we will have to modify the way we control and disburse the information we hold. However, in order to protect the privacy of our citizens, we should change our policies with great care and only after the broadest possible debate.

House Bill No. 2604 may, by itself, be a policy change with limited consequences. However, when viewed in combination with the myriad requests for access to public records that are being introduced into each legislative session, this bill raises serious questions about what our policy should be regarding the commercialization of public records. Our state must develop a clear, comprehensive policy about this issue lest the passage of bills like this one erode away, in a piecemeal fashion, the policy established by the people by initiative in 1972.

In order that a comprehensive policy governing the commercial use of public records can be developed, I will soon appoint a task force to address this issue. Consideration also will be given to issues associated with privacy. This task force will consist of persons who can help advise the executive and legislative branches about this important matter. I will ask the task force to prepare recommendations that can be debated in the 1997 and in subsequent legislative sessions.

By raising the issue this year through the exercise of this veto and others, I am aware that I will be asking our policy makers to undertake a task that will bring into focus a complicated debate that will reveal conflicting values about the public record, privacy, the future of technology, and governmental accountability. However, I am determined that this important debate go forward and that important principles of government not be decided by a process wherein the slow accumulation of exceptions to the underlying law become so extensive that more data is available for commercial uses than is withheld.

For these reasons, I have vetoed House Bill No. 2604 in its entirety.

Respectfully submitted,
Mike Lowry
Governor